НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

КУТОВА МАРИНА АНАТОЛІЇВНА
УДК 351.86:004.056(477)

РОЗВИТОК СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУВАННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Дисертація на здобуття ступеня
доктора філософії

зі спеціальності 281 Публічне управління та адміністрування

галузі знань 28 Публічне управління та адміністрування

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ М.А. Кутова

Науковий керівник
доктор економічних наук, професор
Ткаленко Наталія Валеріївна

Чернігів – 2025

АНОТАЦІЯ

Кутова М.А. Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії зі спеціальності 281 – Публічне управління та адміністрування. Національний університет «Чернігівська політехніка» МОН України, Чернігів, 2025

У дисертації здійснено комплексне теоретико-методичне обґрунтування засад розвитку системи електронного урядування в Україні в умовах цифрової трансформації публічного управління та зростання актуальності інформаційної безпеки як ключового чинника цифрової довіри. На основі аналізу сучасних викликів, міжнародного досвіду та вітчизняної нормативно-правової бази сформовано наукові підходи до удосконалення цифрової взаємодії держави з громадянами, а також розроблено практичні рекомендації щодо підвищення ефективності, прозорості та стійкості цифрових сервісів державного управління.

Структурно-логічна схема дослідження охоплює такі наукові блоки як теоретичний аналіз взаємозв'язку електронного урядування й інформаційної безпеки, емпіричне дослідження сучасного стану цифрового врядування в Україні та обґрунтування стратегічних і практичних напрямів розвитку електронного урядування з урахуванням безпекових аспектів.

Актуальність обраної теми зумовлена необхідністю побудови цілісної та безпечної цифрової екосистеми публічного управління в умовах війни, кіберзагроз і потреби у євроінтеграції. Розвиток електронного урядування сьогодні визначає не лише ефективність адміністративних сервісів, а й здатність держави формувати цифрову довіру, забезпечувати суверенітет у кіберпросторі та адаптувати управлінські механізми до вимог цифровізації.

Метою дисертації є наукове обґрунтування напрямів розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки

України, а також розробка практичних рекомендацій щодо вдосконалення відповідного нормативно-правового забезпечення.

У першому розділі дисертації розкрито сутність, принципи та функції електронного урядування як сучасної форми цифрового публічного управління. Запропоновано розглядати електронне урядування як багатокомпонентну систему, що включає технологічний, нормативно-правовий, інституційний, соціальний та інформаційно-безпековий компоненти. Новизна цього теоретичного удосконалення полягає у комплексному підході, що передбачає системність та адаптивність електронного урядування до викликів цифрової трансформації, зокрема до кіберзагроз. У цьому контексті систематизовано та доповнено основні принципи прозорості, інтерактивності, доступності, ефективності, безпеки, інклюзивності електронного урядування, що створює основу для подальшого розвитку цифрової взаємодії держави і суспільства. Систематизовано функції електронного урядування, зокрема інформаційну, комунікаційну, сервісну, організаційно-управлінську та контрольну. Елементом наукової новизни також є запропонована системна модель взаємозв'язку між електронним урядуванням та інформаційною безпекою, що комплексно охоплює суспільні запити, функціональні завдання електронного урядування, механізми захисту інформації, а також типологію та вплив кіберзагроз на механізми захисту.

Другий розділ присвячено аналізу сучасного стану розвитку електронного урядування в Україні. Проведено оцінку цифровізації органів державної влади, виявлено основні досягнення та основні загрози. Здійснено аналіз національної нормативно-правової бази щодо забезпечення інформаційної безпеки у сфері електронного урядування, що дозволило виявити недоліки чинного законодавства та необхідність його адаптації до сучасних викликів. Окремо проаналізовано характер сучасних загроз інформаційній безпеці, виявлено основні ризики, що стоять перед електронним урядуванням України. Це дозволило глибше усвідомити

пріоритети у державній політиці щодо забезпечення інформаційної безпеки в умовах цифровізації публічного сектору.

Третій розділ присвячений обґрунтуванню стратегічних напрямів розвитку електронного урядування з урахуванням інформаційної безпеки. Запропоновано стратегічну модель планування, яка передбачає горизонтальний поділ стратегічних завдань за часовими періодами на коротко-, середньо- та довгострокову перспективу, з чітким врахуванням динаміки кіберзагроз, ступеня цифрової трансформації та наближення до таких європейських стандартів, як GDPR, NIS2, AI Act. Новизна моделі полягає у комплексному врахуванні безпекових, управлінських і технологічних складових, що відповідає євроінтеграційним прагненням України та забезпечує стійкість і адаптивність електронного урядування до змінюваних умов.

Особливе місце в дисертації займає удосконалення механізму реалізації державної регіональної політики у сфері електронного урядування. Наукова новизна цієї розробки полягає у врахуванні просторової диференціації цифрової інфраструктури, нерівномірності доступу до електронних послуг, регіональних ризиків та загроз інформаційній безпеці. Це дозволяє сформувати інтегровану модель електронного урядування, що базується на принципах цифрової інклюзії, забезпечує інституційну спроможність місцевих органів влади та ефективну взаємодію між центральними та регіональними структурами.

Дисертація також містить практичні рекомендації щодо удосконалення нормативно-правового забезпечення інформаційної безпеки в електронному урядуванні, що поглиблюється конкретизацією напрямів адаптації українського законодавства до європейських стандартів. Запропоновано розширити законодавство шляхом включення принципу нульової довіри, процедур громадського аудиту кібербезпеки та адаптації положень до директиви NIS2 ЄС.

Практичне значення одержаних результатів полягає у можливості їх використання в діяльності органів державної влади та місцевого самоврядування для підвищення ефективності й безпеки цифрового управління та реалізації державної політики у сфері цифрової трансформації.

Ключові слова: електронне урядування, державна служба, цифровізація, інформаційна безпека, кібербезпека, цифрова довіра, публічне управління, цифрові сервіси, нормативно-правове забезпечення.

ABSTRACT

Kutova M.A. Development of the e-government system under ensuring information security of Ukraine - Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in Public Administration (Specialty 281 - Public Management and Administration). Chernihiv Polytechnic National University, Ministry of Education and Science of Ukraine, Chernihiv, 2025.

The dissertation provides a comprehensive theoretical and methodological justification for the development of the e-governance system in Ukraine amidst the digital transformation of public administration and the increasing significance of information security as a key factor in digital trust. Based on the analysis of contemporary challenges, international experience, and the national legal framework, scientific approaches were formulated to enhance digital interaction between the state and citizens. Additionally, practical recommendations were developed to improve the effectiveness, transparency, and resilience of digital public administration services.

The structural and logical framework of the research encompasses several scientific blockssuch as theoretical analysis of the relationship between e-governance and information security; empirical assessment of the current state of digital governance in Ukraine; and strategic and practical justification for the further development of e-governance considering security aspects.

The relevance of the selected topic is driven by the necessity of building a coherent and secure digital ecosystem for public administration under conditions of war, cyber threats, and European integration requirements. Today, the development of e-governance determines not only the efficiency of administrative services but also the state's capacity to build digital trust, ensure sovereignty in cyberspace, and adapt governance mechanisms to digitalization demands.

The aim of the dissertation is to scientifically substantiate directions for the development of the e-governance system in the context of ensuring Ukraine’s information security and to propose practical recommendations for improving relevant legislative and regulatory frameworks.

The first chapter reveals the essence, principles, and functions of e-governance as a modern form of digital public administration. It is proposed to view e-governance as a multi-component system encompassing technological, legal, institutional, social, and informational security components. The novelty of this theoretical enhancement lies in its comprehensive approach, emphasizing systematic and adaptive capacities of e-governance in response to digital transformation challenges, particularly cyber threats. In this context, the key principles - transparency, interactivity, accessibility, efficiency, security, and inclusivity - were systematized and expanded, providing a foundation for further development of digital interaction between state and society. Additionally, the dissertation systematizes the functions of e-governance, including informational, communicative, service-oriented, organizational-management, and supervisory functions. The novelty is further emphasized by the proposed systematic model of the relationship between e-governance and information security, comprehensively integrating societal demands, functional tasks of e-governance, mechanisms of information protection, and typologies and impacts of cyber threats.

The second chapter is dedicated to analyzing the current state of e-governance development in Ukraine. An evaluation of the digitalization of public authorities was conducted, highlighting significant achievements and identifying primary threats. The national legal and regulatory framework concerning information security within

the sphere of e-governance was analyzed, revealing shortcomings and the need for legislative adaptation to contemporary challenges. Additionally, the nature of current information security threats was separately assessed, identifying major risks confronting Ukrainian e-governance. This analysis facilitated deeper understanding and prioritization in state policy regarding information security in the context of public sector digitalization.

The third chapter substantiates strategic directions for the development of e-governance with a focus on information security. A strategic planning model was proposed, incorporating a horizontal division of strategic tasks across short-, medium-, and long-term perspectives, clearly considering the dynamics of cyber threats, the level of digital transformation, and alignment with European standards (GDPR, NIS2, AI Act). The novelty of this model lies in its comprehensive integration of security, managerial, and technological aspects, aligned with Ukraine's European integration aspirations and ensuring resilience and adaptability of e-governance under changing conditions.

Special attention in the dissertation is given to the improvement of mechanisms for implementing state regional policy in the sphere of e-governance. The scientific novelty of this development lies in its consideration of spatial differentiation of digital infrastructure, unequal access to digital services, regional risks, and information security threats. This approach enables the creation of an integrated e-governance model grounded on digital inclusion principles, enhancing institutional capacity of local authorities and promoting effective interaction between central and regional governance structures.

The dissertation also provides practical recommendations for improving legislative and regulatory frameworks concerning information security in e-governance, deepening these recommendations by specifying directions for adapting Ukrainian legislation to European standards. It suggests expanding existing legislation through incorporating the «zero trust» principle, procedures for public cybersecurity audits, and adaptation to the EU's NIS2 Directive.

The practical significance of the obtained results lies in their applicability within public authorities and local self-government bodies, enhancing the efficiency and security of digital governance and implementation of state policy in digital transformation.

Keywords: e-government, civil service, digitalization, information security, cybersecurity, digital trust, public administration, digital services, legal and regulatory framework.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації в наукових фахових виданнях України з публічного управління

1. Kutova M. The framework of information security in e-governance system. Науковий журнал «Economic Synergy», випуск 1(11), 2024. - с.20-30. https://doi.org/10.53920/ES-2024-1-2

2. Кутова М. А. Ідентифікація стратегічних напрямів розвитку системи електронного урядування в контексті інформаційної безпеки. Вісник Хмельницького національного університету. Серія: Економічні науки, 2025, №2. - с.60-63. https://doi.org/10.31891/2307-5740-2025-340-8

3. Кутова М. А. Модель стратегічного планування розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки. Вісник Хмельницького національного університету. Серія: Економічні науки, 2025, №3. – с.12-16. https://doi.org/10.31891/2307-5740-2025-342-3(1)-1

Опубліковані праці апробаційного характеру

4. Кутова М. А. Теоретичні аспекти становлення електронного урядування в Україні. Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). – Чернігів: НУ «Чернігівська політехніка», 2023. – 770 с. (с. 213)

5. Kutova M. Adaptation of e-government and information security strategies to new realities. Юність науки – 2024: збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). – Чернігів: НУ «Чернігівська політехніка», 2024. – 1440 с. (С.192)

6. Kutova M. The impact of political and social factors on the development of E-Government and information security in Ukraine Сучасна парадигма публічного управління : Збірник тез VI Міжнародної науково-практичної конференції (14-16 листопада 2024р.) / [За наук. ред. канд. екон. наук, доц.

Стасишина А.В.]. – Електрон. вид. – Львів : ЛНУ імені Івана Франка, 2025. 930 с. (с.83-84)

7. Кутова М.А. Основні загрози та ризики інформаційної безпеки в електронному урядуванні України. International scientific-practical conference “Economics, accounting, finance and management: strategic priorities for development in the context of globalization”: conference proceedings (Tampere, Finland, March 21, 2025). Tampere, Finland: Scholarly Publisher ICSSH, 2025. 37 pages. (с.30-34).

ЗМІСТ

ВСТУП

Актуальність теми. Цифрова трансформація сучасного світу зумовлює суттєві зміни в організації діяльності органів державної влади та взаємодії з громадянами. Одним із ключових інструментів такого перетворення виступає електронне урядування, яке забезпечує доступність, прозорість та ефективність публічного управління через цифрові технології. Проте, одночасно з поширенням цифрових сервісів зростає і рівень інформаційних ризиків, що ставить на порядок денний питання забезпечення інформаційної безпеки як ключової умови довіри до державних електронних платформ. В умовах війни, загроз кібербезпеці, активізації гібридної агресії, потреба у побудові стійкої системи електронного урядування в Україні, яка базується на високих стандартах захисту даних і цифрової довіри, є надзвичайно актуальною. При цьому, важливим є використання міжнародного досвіду провідних країн, які вже досягли значного прогресу у впровадженні цифрового уряду та побудові комплексної інформаційної безпеки. Потреба у системному аналізі взаємозв'язку між електронним урядуванням і інформаційною безпекою посилюється в умовах таких нових викликів, як широке впровадження хмарних технологій, блокчейн-рішення, штучний інтелект в адмініструванні та масова цифровізація персональних і державних даних. Як підкреслюється у звітах ООН, саме інформаційна безпека стає ключовою умовою формування цифрової довіри, без якої неможливе ефективне функціонування цифрового уряду.

Основне теоретико-методологічне підґрунтя дослідження електронного урядування та цифрової трансформації публічного управління закладене у працях таких провідних зарубіжних учених, як Homburg V. [85], Scholl H. J. [102], Troitiño D. [108], Mazur V. [108], Karokola G. [89], Hoepman J.[76], Fountain J. [83], Norris D. [96], Moon M. [95], West D. [116] та інших. У цих дослідженнях розглядаються питання цифрового уряду як нової управлінської парадигми, проблеми цифрової довіри, публічної участі, використання

штучного інтелекту в адмініструванні, а також безпекові ризики в умовах цифрової взаємодії.

Значний внесок у формування наукових підходів до інформаційної безпеки та інституціонального забезпечення електронного урядування зробили вітчизняні дослідники, зокрема А. Ю. Нашинець-Наумова [49], С. М. Гнатюк [7], Л. С. Харченко [68], В. А. Ліпкан [68], О. М. Степанова [4], В. Н. Дереко [9], А. В. Велігура [4], О. Д. Довгань [10], М. П. Ільницький [28], С. А. Чукут [70], О. В. Загвойська [70], С. О. Гайдученко [6], І. Б. Жиляєв [14], А. І. Семенченко [38], О. М. Руденко [101], І.М. Олійченко [53], та інші вчені, що досліджують проблематику інформаційної безпеки та модернізації публічного управління в Україні.

Попри наявність зазначених досліджень, низка аспектів залишається недостатньо розробленою. Зокрема, не сформульовано цілісну концепцію інформаційної безпеки в електронному урядуванні в умовах гібридної війни та цифрової вразливості держави. Не визначено модель імплементації міжнародного досвіду в українському контексті, з урахуванням правових, інституційних і технічних особливостей. Також потребує визначення напрямів подальшого розвитку електронного урядування на коротко-, середньо- і довгострокові горизонти планування.

Таким чином, тема дослідження є актуальною як у теоретичному, так і в прикладному вимірі. Вона відповідає стратегічним пріоритетам державної політики цифрової трансформації та має значний потенціал для практичного впровадження результатів в органах публічної влади.

Зв’язок роботи з науковими програмами, планами, темами. Дослідження виконувалось у рамках науково-дослідної роботи кафедри менеджменту та адміністрування Національного університету «Чернігівська політехніка» за темою «Механізми державного управління регіональним розвитком в умовах переформатування владних відносин» (номер державної реєстрації 0120U105292), у межах виконання якої автором розроблено механізм реалізації державної регіональної політики у сфері електронного

урядування, який, на відміну від існуючих підходів, враховує територіальну нерівномірність розвитку цифрової інфраструктури, різний рівень доступності електронних послуг для населення, а також регіональні відмінності у ризиках та загрозах інформаційній безпеці

Мета і завдання дослідження. Метою дисертаційної роботи є комплексне теоретико-методологічне обґрунтування напрямів розвитку електронного урядування в контексті забезпечення інформаційної безпеки, а також розроблення практичних рекомендацій щодо вдосконалення нормативно-правового забезпечення електронного урядування.

Для досягнення цієї мети поставлено такі завдання:

- розкрити сутність, принципи та функції електронного урядування як сучасної форми цифрового публічного управління, визначити його місце в контексті розвитку державного управління;

- сформувати теоретичне уявлення про інформаційну безпеку у системі електронного урядування, визначити її ключові елементи, принципи, функціональні характеристики та взаємозв'язок із цифровим управлінням;

- проаналізувати міжнародний досвід забезпечення інформаційної безпеки в електронному урядуванні, виявити кращі світові практики;

- оцінити сучасний стан електронного урядування в Україні, виявити досягнення, недоліки та проблемні зони в його розвитку;

- проаналізувати нормативно-правове забезпечення функціонування електронного урядування в Україні;

- дослідити характер сучасних загроз і ризиків інформаційної безпеки в електронному урядуванні;

- обґрунтувати стратегічні напрями розвитку системи електронного урядування України з урахуванням вимог до інформаційної безпеки, цифрової довіри та інституційної спроможності держави;

- визначити напрями розвитку електронного урядування на регіональному рівні;

- розробити практичні рекомендації щодо вдосконалення нормативно-правового забезпечення інформаційної безпеки в електронному урядуванні.

Об'єктом дослідження є процес розвитку системи електронного урядування в публічному управлінні.

Предметом дослідження є теоретичні, методичні та прикладні засади розвитку електронного урядування в контексті забезпечення інформаційної безпеки в Україні.

Методи дослідження. Теоретико-методологічну основу дисертаційної роботи становить сукупність загальнонаукових і спеціальних методів наукового пізнання, положення теорії державного управління, інформаційної безпеки, цифрової трансформації, а також праці вітчизняних і зарубіжних учених у сфері електронного урядування, кібербезпеки та публічного адміністрування. У дослідженні використано наступні методи:

- загальнофілософський діалектичний метод - для осмислення категорій «електронне урядування», «інформаційна безпека»;

- метод системного аналізу - для дослідження взаємозв'язків між компонентами електронного урядування та інформаційною безпекою;

- абстрактно-логічний метод - для узагальнення понять, формування класифікацій загроз та функціональних елементів цифрової безпеки;

- метод порівняльного аналізу - для зіставлення національної практики з міжнародним досвідом розвитку цифрового уряду та інституційного забезпечення кіберзахисту;

- метод емпіричного аналізу - у тому числі вивчення звітів ООН, Міністерства цифрової трансформації України, CERT-UA, e-Governance Academy, компанії Microsoft, міжнародних цифрових індексів для оцінювання ефективності політик у сфері інформаційної безпеки;

- статистичний аналіз - для визначення рівня цифрової взаємодії держави й громадян, частоти та наслідків кіберінцидентів.

Інформаційну базу дослідження становили вітчизняні та зарубіжні наукові праці, що висвітлюють питання електронного урядування, цифрової

трансформації публічного управління та інформаційної безпеки; нормативно-правові акти України, а саме закони України, укази Президента України, постанови Кабінету Міністрів України, концепції, державні стратегії та дорожні карти цифрової трансформації. Важливу роль відіграли офіційні документи, звіти та методичні матеріали міжнародних організацій, зокрема ООН, Програми розвитку ООН, Світового банку, Європейського Союзу, ОЕСР і т.д.

Інформаційна база також включає офіційні матеріали Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України, Державної служби статистики України. У дослідженні також використано результати впровадження рекомендацій автора у практичну діяльність органів державної влади та місцевого самоврядування, що підтверджено відповідними довідками.

Наукова новизна отриманих результатів. Основні результати дослідження, які формують його наукову новизну і виносяться на захист, полягають у наступному:

удосконалено:

- науково-теоретичне обґрунтування концептуального змісту електронного урядування, яке, на відміну від існуючих, розглядає електронного урядування як інтегровану систему цифрового публічного управління, що поєднує технологічний, нормативно-правовий, інституційний, соціальний та інформаційно-безпековий компоненти та характеризується адаптивністю до викликів цифрової трансформації. Запропоноване удосконалення спрямоване на забезпечення цілісності та системності функціонування цифрових сервісів в умовах зростаючих кіберзагроз і підвищених вимог до безпеки державних інформаційних ресурсів;

- системну модель взаємозв'язку між електронним урядуванням та інформаційною безпекою, яка комплексно поєднує запити суспільства, завдання та функції електронного урядування, компоненти інформаційної безпеки (її складові, механізми захисту, типи загроз), а також відображає

вплив загроз на вибір відповідних механізмів захисту. Це дозволило посилити системність в управлінні цифровими трансформаціями та обґрунтування пріоритетів державної політики у сфері інформаційної безпеки в умовах цифровізації публічного сектору;

- механізм реалізації державної регіональної політики у сфері електронного урядування, що, на відміну від існуючих, враховує просторову диференціацію цифрової інфраструктури, нерівномірність доступу до електронних послуг, а також регіональні асиметрії щодо ризиків і загроз інформаційній безпеці. Запропоноване удосконалення здійснено з метою формування інтегрованого та безпечного електронного урядування, заснованого на принципах цифрової інклюзії, посиленні інституційної спроможності органів місцевого самоврядування та впровадженні багаторівневої моделі управління, що забезпечує узгодженість дій центральних і регіональних органів влади;

набули подальшого розвитку:

- теоретико-методологічне обґрунтування взаємозв'язку між електронним урядуванням та інформаційною безпекою в частині включення категорій «цифрова довіра», «архітектура нульової довіри» та «кіберстійкість» як системоутворюючих понять, що забезпечують концептуальну цілісність електронного урядування, яке, на відміну від фрагментарного підходу в попередніх дослідженнях, грунтується на основі міждисциплінарного аналізу в межах публічного управління, інформаційного права, кібербезпеки та цифрових технологій. Це дозволило сформувати аналітичний концепт для оцінки ефективності цифрових публічних сервісів з урахуванням рівня інформаційної безпеки та довіри громадян;

- модель стратегічного планування розвитку електронного урядування в Україні, в частині запровадження горизонтального поділу стратегічних пріоритетів за часовими періодами (коротко-, середньо- та довгострокова перспектива). Запропонована модель враховує як динаміку загроз інформаційній безпеці, так і індикатори цифрової трансформації, ступінь

наближення до європейських стандартів (GDPR, NIS2, AI Act), а також інституційну спроможність державних органів на різних рівнях. Це дало змогу системно поєднати безпекові, управлінські та технологічні складові розвитку електронного урядування відповідно до євроінтеграційного курсу України;

- пропозиції щодо вдосконалення нормативно-правового забезпечення інформаційної безпеки в електронному урядуванні, які поглиблено через конкретизацію напрямів правової адаптації українського законодавства, що включає розширення змісту Закону України «Про основні засади забезпечення кібербезпеки України» шляхом включення архітектурного принципу нульової довіри як обов'язкової вимоги до публічних ІТ-систем; закріплення процедур громадського аудиту кібербезпеки цифрових сервісів та відкритого контролю за виконанням політик захисту даних; адаптацію положень до вимог Директиви NIS2 Європейського Союзу, у частині захисту критичної інформаційної інфраструктури та стандартизації відповідальності державних органів, що спрямовано на підвищення прозорості, підзвітності та надійності цифрових публічних сервісів в умовах трансформації державного управління.

Практичне значення одержаних результатів полягає в тому, що теоретико-методологіні положення, висновки та науково-практичні рекомендації дослідження становлять концептуальну основу для удосконалення підходів до розвитку електронного урядування в Україні з урахуванням вимог інформаційної безпеки та цифрової довіри. Окремі положення, висновки та рекомендації дослідження були впроваджені в практичну діяльність органів публічної влади, зокрема:

- Центром надання адміністративних послуг Іванівської сільської ради - при впровадженні цифрових рішень у сфері адміністративного обслуговування населення, оптимізації документообігу та підвищенні рівня кіберзахисту (довідка № 305 від 28.04.2025);

- Департаментом інформаційної діяльності та комунікацій з громадськістю Чернігівської обласної державної адміністрації - з метою врахування запропонованих стратегічних підходів у формуванні політики

цифрового розвитку регіону та вдосконаленні інформаційної безпеки в діяльності органів влади (довідка № 01-01-24/4782-вих від 05.05.2025);

- Управлінням адміністративних послуг Чернігівської міської ради - при модернізації інформаційних систем, підвищенні захисту персональних даних та впровадженні електронної ідентифікації громадян у рамках цифрової трансформації адміністративних сервісів (довідка №2354 від 22.05.2025).

- Національним університетом «Чернігівська політехніка» при розробці освітніх компонент «Публічне управління національною та державною безпекою», «Інформаційна політика та електронне врядування» (довідка № 202/08-917/вс від 09.05.2025).

Практична реалізація результатів дослідження сприяє вдосконаленню цифрової взаємодії держави з громадянами, зниженню бюрократичного навантаження, забезпеченню інформаційної безпеки публічних сервісів та підвищенню загального рівня довіри до цифрових сервісів.

Особистий внесок здобувача. Представлена кваліфікаційна наукова праця є результатом самостійного наукового дослідження здобувача. Основні теоретичні положення, аналітичні узагальнення, практичні висновки та науково обґрунтовані пропозиції розроблені автором особисто. При підготовці використано індивідуальний підхід до формування структури дослідження, постановки проблем, вибору методів і інтерпретації результатів. Матеріали публікацій, створених у співавторстві, використані з дотриманням принципів академічної доброчесності, а конкретний внесок здобувача зазначений окремо у списку наукових праць.

Апробація результатів дослідження. Основні положення, теоретичні узагальнення та прикладні результати дисертаційного дослідження доповідалися та обговорювалися на науково-практичних конференціях, зокрема: XIII Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Юність науки - 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства» (м. Чернігів, 26-27 квітня 2023 р.); XIV Міжнародна науково-практична конференція студентів, аспірантів і

молодих вчених «Юність науки - 2024» (м. Чернігів, 24-26 квітня 2024 р.);VI Міжнародна науково-практична конференція «Сучасна парадигма публічного управління» (м. Львів, 14-16 листопада 2024 р.); International scientific-practical conference “Economics, accounting, finance and management: strategic priorities for development in the context of globalization” (м. Тампере, Фінляндія, 21 березня 2025 р.).

Публікації. За результатами дисертації опубліковано 7 наукових праць, з них: 3 статті у наукових фахових виданнях України; 4 публікації у збірниках тез міжнародних науково-практичних конференцій.

Структура і обсяг роботи. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертаційної роботи становить 182 сторінки комп’ютерного тексту, у тому числі основний зміст роботи викладений на 143 сторінках. Робота містить 7 таблиць, 17 рисунків, 5 додатків. Список використаних джерел включає 124 найменування.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ КОНЦЕПТ ВЗАЄМОЗВ'ЯЗКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність, принципи та функції електронного урядування

Електронне урядування є однією з ключових наукових та практичних категорій сучасного етапу розвитку інформаційного суспільства. Воно відображає складну, багаторівневу й динамічну систему взаємодії між різними суб'єктами - державними органами, громадянами, бізнесом, а також громадськими організаціями за допомогою цифрових технологій. У цьому контексті електронне урядування виконує роль не лише інструменту модернізації державного управління, а й чинника трансформації суспільно-політичних відносин.

В умовах стрімкого розвитку інформаційно-комунікаційних технологій електронне урядування постає як ефективний механізм забезпечення відкритості, прозорості та підзвітності державної влади. Його впровадження дозволяє оптимізувати адміністративні процеси, скоротити бюрократичні бар'єри, підвищити якість надання державних послуг та залучити громадян до процесів прийняття управлінських рішень. Електронне урядування виступає інструментом посилення демократичних інститутів і механізмів.

У сучасних наукових дослідженнях виділяють декілька підходів до розуміння електронного урядування [1,6]. Технократичний (технологічний) підхід розглядає електронне урядування як застосування сучасних інформаційно-комунікаційних технологій з метою оптимізації та підвищення ефективності внутрішніх управлінських процесів органів державної влади. В цьому розумінні акцент робиться на технічних рішеннях та інструментах (електронний документообіг, електронні послуги, інтегровані цифрові платформи), що дозволяють скорочувати витрати ресурсів і часу, а також зменшувати бюрократичні процедури [12, 70]. Зокрема, Дубов Д. та Дубова С.

визначають електронне урядування як організацію державного управління з використанням інформаційно-комунікаційних технологій, яка дозволяє ефективніше взаємодіяти державним органам між собою та з суспільством через цифрові канали зв'язку [12].

Значно ширше визначає електронне урядування концептуальний (інституціональний) підхід. Він трактує електронне урядування як комплексну систему, що включає не тільки технології, але й управлінські, соціальні, політичні та нормативно-правові компоненти. Електронне урядування виступає як сучасна управлінська парадигма, спрямована на демократизацію державного управління, посилення прозорості, відкритості, активізацію участі громадян у державних процесах [6, 45, 38, 70]. Гайдученко С. описує електронне урядування як систему, що забезпечує прозору та відкриту взаємодію влади з громадянами і сприяє формуванню довіри до державних органів через надання доступних і якісних адміністративних послуг [38, 54].

У межах адміністративно-правового підходу електронне урядування аналізується як сукупність правових норм і адміністративних практик, що регулюють використання інформаційно-комунікаційних технологій у діяльності державних органів. Важливий акцент робиться на забезпеченні інформаційної безпеки, захисту персональних даних та створенні належних умов для використання електронних технологій у правовому полі держави [1, 38]. Так, Александрова М. розглядає електронне урядування як інструмент адміністративно-правового забезпечення інформаційної безпеки та впровадження сучасних форм управління, які відповідають національним та міжнародним стандартам [1].

Натомість, соціально-демократичний підхід підкреслює роль електронного урядування як інструмента розширення демократичних прав і свобод громадян. Акцентується увага на електронних інструментах демократії - електронних голосуваннях, петиціях, консультаціях, які сприяють підвищенню громадянської активності і безпосередньої участі громадян у формуванні державної політики та управлінні суспільними процесами [38, 70].

Чукут С., Загвойська О. і Цимбаленко Я. наголошують на ролі електронного урядування у розвитку електронної демократії, завдяки чому громадяни мають змогу безпосередньо брати участь у прийнятті рішень на державному рівні через електронні засоби [70].

І, нарешті, інтегративний підхід представляє електронне урядування як багатовимірний феномен, що поєднує в собі всі вищезазначені аспекти. Він наголошує, що ефективне функціонування електронного урядування можливе лише за умови комплексного підходу, де технологічні рішення інтегруються з адміністративно-правовими механізмами, демократичними інструментами та соціальними практиками з метою формування сучасної, ефективної та відкритої держави [38, 70]. Так, у роботі «Концептуальні засади розвитку електронного урядування в Україні» електронне урядування визначається як комплексний підхід, що передбачає широке застосування інформаційно-комунікаційних технологій для створення відкритої, прозорої і ефективної системи державного управління, яка забезпечує якісну взаємодію між державою, громадянами та бізнесом [38]. В таблиці 1.1 наведено окремі визначення вітчизняних та іноземних дослідників електронного урядування в контексті окремих підходів, а також визначення яке міститься в Концепції розвитку електронного урядування в Україні [39]. Електронне урядування сприяє формуванню інноваційного середовища в публічному секторі, що відповідає сучасним вимогам сталого розвитку [1, 6, 14, 37, 38].

Таблиця 1.1. Визначення електронного урядування в контексті наукових підходів

Підхід	Автор, назва праці та посилання	Визначення електронного урядування
1	2	3
Технократичний	Jane Fountain, «Building the Virtual State: Information Technology and Institutional Change» [83]	Процес впровадження технологічних рішень у публічному секторі для покращення управління, взаємодії та ефективності надання послуг.
	Donald Norris, «E-Government: Revolution or Evolution?» [96]	Застосування ІКТ в органах влади для підвищення ефективності державного управління, доступності послуг та взаємодії з громадськістю.
	M. Jae Moon, «The Evolution of E-Government among Municipalities» [95]	Використання ІКТ в урядових установах для вдосконалення державного управління, прозорості та взаємодії з громадянами.
Концептуальний	Бакуменко В., «Електронне урядування як складова сучасного державного управління» [2]	Сукупність процесів управління та взаємодії між державою і суспільством, що реалізуються через ІКТ для забезпечення прозорості та ефективності державного управління.
	Darrell West, «Digital Government: Technology and Public Sector Performance» [116]	Інтеграція інформаційних технологій у процеси управління з метою підвищення якості адміністративних послуг та активізації громадянської участі.
Адміністративно-правовий	Ільницький М., «Адміністративно-правові засади електронного урядування у сфері публічного управління в Україні» [28]	Система, що базується на адміністративно-правових нормах, які забезпечують публічно-правові інтереси та організують управлінські відносини в сфері публічного управління.

Продовження табл.1.1.

1	2	3
Соціально-демократичний	Guy Peters, «Handbook of Public Administration»	Система управління, яка завдяки використанню цифрових технологій сприяє трансформації моделей взаємодії громадян із державою, забезпечуючи більшу громадську участь і демократичність процесів ухвалення рішень.
	Концепції розвитку електронного урядування в Україні [39]	«Форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян»
Інтегративний	Ющенко Н. В. «Електронне урядування в Україні: стан та перспективи розвитку» [73]	Комплексна система державного управління, що базується на ІКТ, спрямована на забезпечення прозорості, ефективності та доступності державних послуг, покращення демократизації та антикорупційної діяльності.
	Чукут С. А., Загвойська О. В., Цимбаленко Я. Ю. «Основи електронного урядування» [70]	Система організації державного управління, що забезпечує інтерактивну взаємодію влади з громадянами, бізнесом та іншими зацікавленими сторонами за допомогою сучасних ІКТ
	United Nations E-Government Survey 2024 [114]	Уряд, який, використовуючи інформаційно-комунікаційні технології, надає громадянам та підприємствам можливість взаємодіяти з урядом, використовуючи різноманітні електронні засоби масової інформації

Джерело: систематизовано та побудовано автором

Важливим аспектом розуміння сутності електронного урядування є диференціація похідних термінів, таких як електронний уряд (e-government), електронне урядування (e-governance) та цифровий уряд (digital government). Ці поняття є взаємопов'язаними, проте відображають різні аспекти та ступені цифровізації процесів на рівні державних структур (рис.1.1).

Рисунок 1.1. Теоретичний конструкт взаємозв'язку похідних термінів електронного урядування

Джерело: побудовано автором

Взаємозв'язок між цими поняттями можна охарактеризувати як поступову еволюцію - від початкової автоматизації внутрішніх процесів (електронний уряд), через ширше залучення громадськості та демократизацію управлінських процесів (електронне урядування), до повної цифровізації і

застосування передових технологій для максимального підвищення ефективності, прозорості та громадської участі (цифровий уряд).

Поняття електронного уряду, як правило, розглядається у вузькому технічному сенсі. Воно описує процес впровадження інформаційно-комунікаційних технологій у повсякденну діяльність органів державної влади, переважно орієнтований на внутрішні потреби державних структур. Основною метою електронного уряду є оптимізація адміністративних процесів, підвищення продуктивності праці державних службовців, скорочення витрат часу і ресурсів при наданні послуг громадянам і бізнесу. Важливою ознакою електронного уряду є автоматизація документообігу, створення єдиних баз даних і цифрових реєстрів, а також впровадження електронних послуг з обмеженим рівнем взаємодії з громадськістю [12, 14].

Натомість електронне урядування представляє собою значно ширше поняття. Окрім технологічної складової, воно охоплює демократичні процеси, такі як активна участь громадян у формуванні державної політики, використання цифрових платформ для публічних консультацій, голосувань, збору думок і зворотного зв'язку. У цьому контексті електронне урядування є інструментом не лише адміністративної, але й політичної діяльності, оскільки сприяє підвищенню прозорості, відкритості та підзвітності державних органів перед суспільством. Завдяки електронному урядуванню громадяни отримують реальні можливості впливати на прийняття рішень, а держава - встановлювати якісно новий рівень комунікації та довіри з громадянами і бізнесом [1, 6, 38].

Термін цифровий уряд описує найбільш сучасний і комплексний етап розвитку електронного урядування, орієнтований на повну цифрову трансформацію державних структур і процесів. Цифровий уряд передбачає глибоке впровадження новітніх технологій, таких як штучний інтелект, хмарні сервіси, великі дані, блокчейн та Інтернет речей. Метою цифрового уряду є створення інтегрованих інформаційних систем, здатних у режимі реального часу надавати персоналізовані державні послуги, забезпечувати високий рівень інформаційної безпеки, здійснювати глибокий аналіз даних для

прийняття управлінських рішень, а також максимально автоматизувати адміністративні та управлінські процедури [14,70,111]. Цифровий уряд характеризується не лише технологічною досконалістю, але й максимальною орієнтацією на потреби та інтереси громадян, забезпечуючи принципово новий рівень взаємодії між державою, суспільством і бізнесом [14,70]. Порівняльна характеристика електронного уряду, електронного урядування і цифрового уряду систематизована в таблиці 1.2.

Узагальнюючи наукові підходи, електронне урядування можна визначити як організацію системи державного управління на основі широкого використання інформаційно-комунікаційних технологій. Метою цього процесу є підвищення ефективності, відкритості та прозорості діяльності органів державної влади, забезпечення якісного надання адміністративних послуг, а також покращення умов для реалізації громадянських прав і свобод. В контексті всебічності нашого дослідженні необхідно приділити увагу основним завданням електронного урядування. У наукових доробках вітчизняних науковців [1, 6, 12, 14, 38, 70] з галузі знань публічного управління та адміністрування можна знайти чотири основні завдання (рис.1.2).

Цифрова взаємодія держави, громадян та бізнесу полягає у забезпеченні ефективної комунікації та обміну інформацією між учасниками процесу управління за допомогою цифрових технологій, що дозволяє скорочувати час, зменшувати витрати та підвищувати якість послуг [6, 12, 38, 70].

Прозорість та відкритість процесів управління забезпечує доступності інформації про діяльність органів влади, яка дозволяє громадянам та бізнесу контролювати владу, попереджувати корупцію та підвищувати рівень довіри до державних органів [1, 14, 38].

Орієнтація на потреби громадян - це надання послуг, які максимально враховують індивідуальні потреби та побажання громадян, що сприяє підвищенню задоволеності населення державними послугами та посиленню громадянської активності [6, 14, 70].

Таблиця 1.2. Порівняльна характеристика похідних термінів електронного урядування

Критерій	Електронний уряд	Електронне урядування	Цифровий уряд
Ціль	Початкова стадія цифровізації публічних сервісів	Автоматизація надання державних послуг	Інноваційна трансформація державного управління
Технічна основа	Використання базових ІКТ для онлайн-доступу	Інтернет-технології, веб-портали	Хмарні технології, ШІ, великі дані, блокчейн
Рівень інтеграції	Відокремлені ініціативи в межах окремих органів	Обмежена інтеграція між установами	Високий рівень міжвідомчої інтеграції
Орієнтація на користувача	Обмежена взаємодія з користувачем	Обмежена, часто односпрямована комунікація	Центральна роль користувача в дизайні сервісів
Участь громадян	Орієнтація на інформування громадян	Пасивне споживання інформації	Активна участь через е-голосування, консультації, петиції
Використання інноваційних технологій	Впровадження базових цифрових сервісів	Мінімальне або фрагментарне	Широке впровадження AI, аналітики, IoT
Підхід до інформаційної безпеки	Захист на рівні окремих сервісів	Фрагментарний захист систем і даних	Інституційний підхід до управління ризиками, довірою та приватністю
Підтримка Цілей сталого розвитку (SDG)	Непрямий вплив через підвищення доступності послуг	Опосередкований внесок у цілі стійкого розвитку (SDG)	Безпосередня підтримка SDG 9, 16, 17

Джерело: систематизовано та побудовано автором

Рисунок 1.2. Основні завдання електронного урядування

Джерело: побудовано автором на основі [1, 6, 12, 14, 38, 70]

І, нарешті, зменшення бюрократичних процедур, як автоматизація адміністративних процесів, що дозволяє скорочувати кількість процедур, витрати часу і ресурсів на отримання адміністративних послуг, підвищувати їх доступність і зручність для користувачів [1, 12, 14]. Чітко визначені завдання дозволяють суттєво підвищити ефективність державного управління, зменшити корупцію, посилити довіру громадян до влади і створити сприятливе середовище для розвитку демократичних інститутів та громадянського суспільства. Електронне урядування є не лише технологічним інструментом, а фундаментальним фактором модернізації державного

управління, що визначає майбутній вектор розвитку сучасних держав у глобальному інформаційному суспільстві.

Для реалізації визначених основних завдань електронного урядування необхідно чітко розуміти основні принципи які визначають сутність та специфіку взаємодії між державою, громадянами та бізнесом у цифровому середовищі. Серед найбільш обговорюваних принципів у науковій літературі є прозорість та відкритість, інтерактивність, доступність, ефективність, безпека та конфіденційність, а також інклюзивність.

Прозорість та відкритість розглядається як основний принцип, який забезпечує громадянам вільний доступ до інформації про діяльність органів влади. Гайдученко С. підкреслює, що саме цей принцип сприяє формуванню довіри населення до державних структур, попередженню корупційних ризиків та підвищенню відповідальності посадовців [6]. Також Семенченко А. та Жиляєв І. зазначають, що прозорість процесів прийняття рішень є передумовою демократизації управління та суспільного контролю за діяльністю органів влади [14, 38].

Інтерактивність передбачає зворотний зв’язок між владою та громадянами, забезпечуючи активну участь останніх у процесах управління. За словами Норріса Д., інтерактивність трансформує звичайні адміністративні процедури в активну двосторонню взаємодію, де громадяни стають повноцінними учасниками прийняття рішень [96]. Цю думку поділяють і Семенченко А. з Жиляєвим І., які підкреслюють, що цифрові технології відкривають нові можливості для ефективної комунікації влади з суспільством [14].

Доступність означає рівні можливості для всіх громадян користуватися державними цифровими послугами незалежно від соціально-економічного статусу чи місця проживання. У звіті ООН зазначено, що доступність передбачає не лише технологічні аспекти, але й створення рівних умов для всіх верств населення, включаючи тих, хто знаходиться у віддалених районах або має особливі потреби [111]. Дубов Д. та Дубова С. також зазначають, що саме

доступність є важливим чинником реалізації принципів соціальної справедливості в умовах цифровізації [12].

Ефективність передбачає скорочення витрат часу і ресурсів шляхом оптимізації адміністративних процедур. На думку Муна М., ефективність забезпечується завдяки впровадженню автоматизації та цифровізації процесів, що дозволяє значно покращити якість надання державних послуг і підвищити продуктивність державних органів [95]. Подібні ідеї висловлює Фаунтейн Дж., яка акцентує увагу на здатності електронних технологій трансформувати традиційні бюрократичні механізми у більш ефективні системи управління [83].

Безпека та конфіденційність є критично важливими для забезпечення довіри до електронного урядування. Александрова М. вказує, що гарантія інформаційної безпеки та захист персональних даних є необхідними передумовами для широкого впровадження електронних послуг та підтримки громадської довіри [1]. В цьому контексті звіт ООН також наголошує на важливості створення надійних систем захисту інформації від кіберзагроз [111].

Інклюзивність передбачає залучення всіх соціальних груп до використання електронних послуг, особливо людей з особливими потребами. У доповіді ООН інклюзивність трактується як створення умов, які дозволяють всім громадянам, незалежно від їхніх фізичних, соціальних чи економічних особливостей, отримувати доступ до державних послуг [111]. Ющенко Н. наголошує на необхідності розробки спеціальних інтерфейсів і адаптивних платформ, що враховують потреби вразливих категорій населення, забезпечуючи їх інтеграцію у цифрове суспільство [73]. Представлений аналіз різних авторських позицій дозволяє стверджувати, що принципи електронного урядування є фундаментальними орієнтирами для формування ефективної, відкритої та інклюзивної цифрової держави, здатної ефективно взаємодіяти із суспільством та відповідати на виклики сучасного інформаційного середовища.

Інструментами, за допомогою яких держава реалізує політику у сфері інформаційного суспільства, забезпечуючи ефективну взаємодію з громадянами та бізнесом ми можемо ідентифікувати як функції електронного урядування (рис.1.3). Серед яких основними є інформаційна, комунікаційна, сервісна, організаційно-управлінська та контрольна функції [111].

Інформаційна функція полягає в забезпеченні відкритості інформації про діяльність державних органів, доступності публічних даних, а також інформуванні про державні послуги та ініціативи [111]. Завдяки електронним ресурсам державні органи надають громадянам доступ до актуальної інформації, що забезпечує прозорість та відкритість влади, сприяє формуванню довіри громадян. Як зазначають деякі автори [12], важливим елементом інформаційної функції є поширення відкритих даних, що дозволяє громадськості ефективно контролювати діяльність держави та брати активну участь у формуванні політик.

Комунікаційна функція забезпечує інтерактивну взаємодію влади з громадянами, використовуючи цифрові технології для організації консультацій, опитувань, електронних голосувань та інших форм двосторонньої комунікації. В звіті ООН [111] наголошується на тому, що така інтерактивність дозволяє громадянам не лише отримувати інформацію, а й активно впливати на процеси ухвалення рішень, що значно покращує якість державного управління. Також вказується, що активна комунікація влади з громадянами сприяє підвищенню ефективності державного управління та залученню населення до суспільно важливих процесів [6]. Ще одна, сервісна, функція охоплює надання адміністративних послуг у цифровому форматі (електронні послуги, е-послуги), що значно спрощує взаємодію громадян і бізнесу з державними установами. Наприклад, реєстрація бізнесу, подання декларацій та заявок на отримання соціальних послуг дедалі частіше реалізуються онлайн, що суттєво зменшує витрати часу та ресурсів громадян. Це дозволяє зменшити адміністративний тягар та підвищити зручність взаємодії громадян з органами влади [1, 111]

Рисунок 1.3. Функції системи електронного урядування

Джерело: побудовано автором на основі [12, 38, 70]

Організаційно-управлінська функція передбачає цифровізацію внутрішніх процесів у державних органах. Це стосується впровадження систем електронного документообігу, створення цифрових офісів та автоматизації управлінських процедур, що дозволяє значно скоротити час на прийняття рішень та підвищити ефективність роботи органів влади [12]. Зокрема, Александрова М. наголошує, що впровадження таких технологій сприяє зменшенню бюрократичних процедур, покращенню міжвідомчої координації та більш якісному виконанню управлінських завдань [1].

Контрольна функція електронного урядування реалізується через використання сучасних цифрових технологій для моніторингу та оцінювання ефективності діяльності державних органів. За допомогою цифрових платформ громадяни можуть здійснювати громадський контроль, подаючи онлайн-скарги та повідомлення про порушення, що стимулює прозорість і відповідальність державних службовців. Ільницький М. вважає, що ефективний електронний контроль сприяє підвищенню відповідальності та підзвітності влади, запобігаючи корупції та зловживанням службовими повноваженнями [28].

Аналіз сутності, принципів та функцій електронного урядування дозволяє зробити висновок, що ефективна реалізація цього феномену потребує системного підходу та всебічного врахування різноманітних аспектів. Впровадження електронного урядування на сучасному етапі розвитку суспільства пов'язано не лише з перевагами цифровізації адміністративних процедур, але й зі значними викликами щодо забезпечення надійності та безпеки інформаційних ресурсів і персональних даних громадян. У цьому контексті постає нагальна необхідність детального вивчення теоретичних аспектів інформаційної безпеки як одного з ключових компонентів системи електронного урядування. Саме тому важливою умовою ефективного функціонування електронного урядування є створення і підтримання належних механізмів забезпечення інформаційної безпеки, що буде розглянуто в наступному пункті нашого дослідження.

Розглянуті аспекти електронного урядування демонструють його складну, багаторівневу природу, яка не обмежується лише технологічним впровадженням інформаційних систем та оптимізацією управлінських процесів. В умовах постійного зростання цифрових загроз і ризиків, важливо підкреслити, що безпека інформаційного середовища стає ключовим фактором стабільного функціонування та розвитку системи електронного урядування. У зв'язку з цим, виникає необхідність уточнення визначення електронного урядування з урахуванням аспекту інформаційної безпеки. Ми пропонуємо трактувати поняття ***«електронне урядування» як інтегровану систему державного управління, засновану на застосуванні сучасних інформаційно-комунікаційних технологій, що спрямована на підвищення ефективності, прозорості та відкритості взаємодії між державою, громадянами та бізнесом на основі використання механізмів забезпечення захисту інформації, гарантування конфіденційності та цілісності персональних даних та інформаційних ресурсів держави.***

Запропоноване визначення акцентує увагу на взаємозв'язку між цифровою трансформацією державного управління та необхідністю забезпечення високих стандартів інформаційної безпеки, підкреслюючи, що успішна реалізація електронного урядування є неможливою без надійного захисту інформаційних активів.

Все вище згадане в даному підпункті дозволяє зробити висновок, що ефективна реалізація феномену електронного урядування потребує системного підходу та всебічного врахування різноманітних аспектів. Впровадження електронного урядування на сучасному етапі розвитку суспільства пов'язано не лише з перевагами цифровізації адміністративних процедур, але й зі значними викликами щодо забезпечення надійності та безпеки інформаційних ресурсів і персональних даних громадян. У цьому контексті постає нагальна необхідність детального вивчення теоретичних аспектів інформаційної безпеки як одного з ключових компонентів системи електронного урядування. Саме тому важливою умовою ефективного

функціонування електронного урядування є створення і підтримання належних механізмів забезпечення інформаційної безпеки, що буде розглянуто в наступному пункті нашого дослідження.

1.2. Теоретичні аспекти інформаційної безпеки в електронному урядуванні

Проблематика інформаційної безпеки є особливо актуальною в умовах активного розвитку інформаційного суспільства та поширення цифрових технологій, зокрема у сфері електронного урядування. За сучасними підходами інформаційна безпека трактується як комплексний стан захищеності інформаційного середовища держави, при якому гарантується конфіденційність, цілісність і доступність інформації, а також її надійний захист від внутрішніх і зовнішніх загроз [4, 9, 32, 49, 58].

Попри наявність численних підходів до трактування поняття «інформаційна безпека», на сьогоднішній день у науковій спільноті не існує єдиного універсального визначення цього терміну. Різні дослідники акцентують увагу на окремих аспектах, що зумовлює багатогранність інтерпретацій та складність уніфікації підходів до цього поняття.

Так, на думку Нашинець-Наумової А., інформаційна безпека, перш за все, має розглядатися у контексті правового регулювання. Авторка підкреслює, що ефективне забезпечення інформаційної безпеки потребує створення спеціального правового режиму, який би дозволяв системно та цілеспрямовано здійснювати захист національних інформаційних ресурсів. Такий режим, на її переконання, має охоплювати широкий спектр відносин, що виникають у сфері обігу інформації, зокрема забезпечувати охорону інтересів громадян, суспільства та держави загалом. У цьому контексті інформаційна безпека постає як правова категорія, тісно пов’язана із питаннями національного суверенітету, прав і свобод людини, а також функціонування державних інституцій у цифровому середовищі [49].

Подібну точку зору висловлює Дереко В. [9], який, однак, розширює розуміння інформаційної безпеки, включаючи до нього не лише правові, а й технічні, організаційні, соціальні та політичні складові. Він зазначає, що інформаційна безпека - це комплексна система заходів, яка передбачає не лише захист інформаційних систем від зовнішнього втручання чи витоку даних, але й активну роботу із запобігання поширенню деструктивної інформації, протидію інформаційним впливам, які можуть мати негативні наслідки для громадської думки, національної безпеки або політичної стабільності [9]. Таким чином, інформаційна безпека розглядається ним як складний багатовимірний феномен, що потребує інтеграції зусиль на різних рівнях - від технічного адміністрування до формування державної інформаційної політики.

Згідно з позицією Довганя О., сучасні інформаційні структури, які активно використовуються в діяльності держави, становлять основу для забезпечення належного рівня інформаційної безпеки [10]. Ці структури виконують не лише функцію підтримки комунікацій та обміну інформацією в межах державного управління, а й виступають критично важливими інструментами для реалізації управлінських рішень у цифровому середовищі. У зв’язку з цим наголошується на необхідності постійного оновлення та модернізації зазначених систем, що зумовлено динамічним розвитком інформаційних технологій та постійною еволюцією потенційних загроз у сфері кібербезпеки. Застарілі інформаційні інфраструктури можуть стати вразливими до кіберзлочинності, технічних збоїв або цілеспрямованих атак, що створює ризики для стабільного функціонування електронних систем управління та, в ширшому контексті, для безпеки держави загалом [11].

У цьому ж контексті Домбровська С. і Полторак С. підкреслюють, що забезпечення ефективної інформаційної безпеки неможливе без всебічного підходу до формування стратегії безпеки держави [11]. Вони зазначають, що ключовим елементом цієї стратегії має бути впровадження дієвих механізмів, які б дозволяли не лише реагувати на наявні загрози, але й передбачати

потенційні ризики, що виникають у цифровому середовищі. На думку авторів, такі механізми мають включати як нормативно-правові інструменти - тобто розробку законодавчої бази, яка регулює захист інформації, - так і технічні засоби захисту, зокрема інструменти шифрування, системи виявлення вторгнень, програмні засоби контролю доступу та інші технологічні рішення, що дозволяють забезпечити безперервність, цілісність і конфіденційність інформаційних потоків [11].

Окремої уваги потребує питання інформаційної безпеки в умовах розширення електронного урядування, оскільки цифровізація управлінських процесів зумовлює появу нових викликів та ризиків. Велігура А. та інші дослідники зазначають, що в умовах цифрової трансформації державного управління особливої актуальності набуває захист інформаційних систем органів влади [4]. Вони мають бути надійно захищені від кібератак, несанкціонованого втручання, витоку конфіденційної інформації та інших форм цифрових загроз. Зокрема, йдеться про захист серверної інфраструктури, баз даних, каналів передачі інформації, а також цифрових платформ, які забезпечують взаємодію між громадянами і державою [4].

Не менш важливим компонентом інформаційної безпеки в електронному урядуванні є захист персональних даних громадян. З огляду на широке використання цифрових технологій для збору, обробки і зберігання особистої інформації, держава зобов’язана забезпечити її захист на найвищому рівні. Це передбачає відповідність національних стандартів захисту персональних даних міжнародним нормам, зокрема таким, як Загальний регламент про захист даних Європейського Союзу (General Data Protection Regulation of the European Union) [84], та впровадження сучасних технологічних рішень, які дозволяють мінімізувати ризики витоку або несанкціонованого доступу до особистої інформації [74, 104]. У цьому контексті важливою є не лише технічна, але й етична складова, яка передбачає прозорість у поводженні з персональними даними, інформування громадян

про способи їх використання та забезпечення механізмів контролю з боку користувачів.

Сучасне розуміння інформаційної безпеки в державному управлінні виходить далеко за межі традиційного уявлення про технічний захист. Воно охоплює широкий спектр заходів - від оновлення інформаційної інфраструктури до правового регулювання, від протидії кіберзагрозам до етичного управління персональними даними, - що вимагає комплексного, міждисциплінарного підходу до формування національної політики у сфері інформаційної безпеки. Зарубіжний досвід переконливо свідчить про те, що забезпечення інформаційної безпеки в електронному урядуванні вимагає цілісного та комплексного підходу, який охоплює не лише технічні аспекти, а й організаційні, правові та етичні механізми. Так, Ахмед Д., аналізуючи досвід різних країн у сфері захисту персональних даних у межах систем електронного урядування, підкреслює критичну необхідність розробки та впровадження ефективних політик управління інформаційними ризиками [74]. Автор зазначає, що такі політики мають охоплювати чітко визначені процедури виявлення, аналізу, оцінки та мінімізації ризиків, пов’язаних з обробкою персональних даних. Зокрема, йдеться про ризики витоку інформації, несанкціонованого доступу, а також зловживання інформацією з боку внутрішніх користувачів. Успішне управління цими ризиками потребує не лише наявності відповідного програмного забезпечення, а й належної підготовки персоналу, системи внутрішнього аудиту та інституційного контролю [74].

Росс Р. [100] у своїх дослідженнях підкреслює, що рівень надійності та стійкості інформаційних систем у сфері державного управління безпосередньо залежить від регулярного моніторингу та оцінки ефективності заходів, які впроваджуються для забезпечення інформаційної безпеки. Вони розглядають інформаційну безпеку як систему, що складається з трьох ключових типів контролю: технічного (включаючи антивірусне програмне забезпечення, системи шифрування тощо), адміністративного (встановлення політик, правил

доступу, розподілу повноважень) та фізичного (обмеження фізичного доступу до серверів, приміщень, де зберігаються критичні дані) [100]. Автори наполягають на необхідності систематичного перегляду цих заходів, а також на використанні методів тестування на проникнення і симуляцій інцидентів для виявлення вразливих місць у системах [100].

Сільва Дж. та його колеги, здійснюючи глобальний порівняльний огляд практик електронного урядування, роблять акцент на важливості інформаційної безпеки як ключового чинника формування громадської довіри до цифрових сервісів, які надаються державними структурами [104]. На основі аналізу досвіду різних країн, автори доводять, що наявність ефективної системи кіберзахисту безпосередньо корелює з рівнем готовності громадян користуватися онлайн-послугами держави. Зокрема, якщо громадяни відчувають, що їхні персональні дані можуть бути недостатньо захищені, це призводить до зниження рівня цифрової взаємодії, зростання недовіри до державних інституцій і, в деяких випадках, до повернення до традиційних, офлайн-форм комунікації. Отже, автори підкреслюють, що інформаційна безпека повинна бути не лише технічним пріоритетом, а й частиною політики цифрової довіри, що охоплює питання прозорості, підзвітності та взаємодії з громадянами [30].

Комплексне забезпечення інформаційної безпеки є передумовою стабільного функціонування державних електронних послуг і формування довіри громадян до органів державної влади. У наукових джерелах [4, 49, 99] зазначається, що інформаційна безпека складається з декількох взаємопов’язаних та взаємодоповнюючих елементів, серед яких традиційно виокремлюють конфіденційність, цілісність та доступність інформації. Конфіденційність інформації визначають як стан, при якому інформація захищена від несанкціонованого доступу і використовується тільки тими особами, які мають відповідні повноваження [4, 49, 115]. Конфіденційність особливо важлива в системах електронного урядування, де обробляються значні обсяги персональних та державних даних, доступ до яких суворо

регламентований законодавчими актами та внутрішніми регламентами [31, 68, 90]. Нашинець-Наумова А. наголошує, що забезпечення конфіденційності вимагає комплексного підходу, що включає як нормативно-правові акти, так і технічні засоби захисту інформації, зокрема криптографічні методи захисту [49].

Цілісність інформації передбачає її захищеність від несанкціонованого втручання, внесення змін або викривлень. Це гарантує, що інформація, яка циркулює в системі електронного урядування, залишається автентичною та надійною для використання у процесах прийняття управлінських рішень [10, 30, 119]. На думку Дереко В., порушення цілісності інформації може призводити до значних ризиків, оскільки ухвалення управлінських рішень на основі викривлених або неповних даних може мати серйозні наслідки для суспільства та держави [9]. Саме тому для забезпечення цілісності інформації застосовуються механізми контролю та верифікації даних на усіх рівнях електронного документообігу [4, 92, 100].

В свою чергу, доступність інформації має на меті забезпечення своєчасного і безперешкодного доступу уповноважених користувачів до інформаційних ресурсів та систем. Згідно з твердженням Довганя О., цей елемент є критично важливим для ефективної роботи державних органів, оскільки він гарантує безперервність функціонування системи електронного урядування та оперативність у процесі ухвалення рішень [10]. Велігура А., Дегтярьова Л. та Степанова О. вважають, що забезпечення доступності вимагає впровадження стійких до збоїв і атак інформаційних технологій, регулярного резервування інформації та постійного моніторингу стану інформаційних ресурсів [4].

Крім трьох основних елементів, низка авторів також додає такі характеристики, як автентичність та підзвітність інформації [74, 104]. Окремі дослідженнях наголошують, що автентичність забезпечує точність і коректність інформації, а також підтверджує її походження, що особливо важливо для систем електронного урядування [74]. Підзвітність інформації, на

думку Росс Р. та інших авторів, забезпечується шляхом впровадження контролю за доступом, ведення журналів подій і регулярних аудитів безпеки, що дозволяє встановити відповідальність за порушення правил роботи з інформаційними ресурсами [100]. Від ефективності реалізації зазначених елементів безпосередньо залежить рівень довіри громадян і бізнесу до електронних послуг держави, що визначає загальний успіх процесу цифровізації державного управління.

Отже, визначивши основні складові інформаційної безпеки - конфіденційність, цілісність, доступність, автентичність та підзвітність - необхідно підкреслити, що їх ефективна реалізація суттєво залежить від специфіки та умов сучасного цифрового середовища. В умовах активної цифровізації державного управління з'являються нові виклики й загрози, що потребують переосмислення підходів до інформаційної безпеки, а також адаптації традиційних механізмів захисту інформації до сучасних технологічних реалій.

Рисунок 1.4 демонструє комплексний підхід до забезпечення інформаційної безпеки в електронному урядуванні, який включає правові, організаційні та технічні заходи. Ці заходи спрямовані на забезпечення основних складових інформаційної безпеки - конфіденційності, цілісності, доступності, автентичності та підзвітності інформації. Процес цифровізації державного управління супроводжується істотними змінами в системі забезпечення інформаційної безпеки, оскільки він передбачає впровадження новітніх інформаційно-комунікаційних технологій, використання електронних платформ для взаємодії між державними органами, громадянами та бізнесом. У цих умовах виникають нові виклики, пов'язані з ризиками несанкціонованого доступу, кібератаками, витоком інформації та зловживанням персональними даними [49, 4, 68].

Рисунок 1.4. Структурно-функціональна модель інформаційної безпеки в системі електронного урядування

Джерело: побудовано автором на основі [4,19,10,11]

Однією з ключових особливостей сучасного підходу до забезпечення інформаційної безпеки в електронному урядуванні є усвідомлення необхідності впровадження комплексного та міждисциплінарного підходу до захисту інформації. Це означає, що жодна окрема категорія заходів, чи то технічна, правова або організаційна, не може бути ефективно ізольовано від

інших. Усі ці компоненти мають діяти скоординовано в межах єдиної стратегії, що забезпечує стійкість державних цифрових систем до внутрішніх і зовнішніх загроз.

На думку Велігури А. та його співавторів, інформаційна безпека в умовах електронного урядування не може бути ефективною без системної інтеграції правових, організаційних, технічних та освітніх заходів [4]. Автори наголошують, що правова складова повинна передбачати чітке регулювання порядку обробки інформації, відповідальності за порушення інформаційної безпеки, а також механізми контролю з боку держави. Організаційний компонент включає розробку внутрішніх політик, створення профільних структур, визначення ролей і повноважень працівників. Технічна складова охоплює впровадження сучасних систем захисту, а освітній компонент - підготовку кваліфікованих кадрів, що здатні ефективно реагувати на інформаційні загрози та забезпечувати стабільне функціонування систем [4].

У зв’язку з інтенсивною цифровізацією державного сектору особливого значення набуває впровадження сучасних технологій захисту інформації. До найбільш ефективних на сьогодні методів належать криптографічний захист даних, який гарантує цілісність і конфіденційність інформації; багатофакторна аутентифікація, що значно ускладнює несанкціонований доступ до систем; технології блокчейн, які забезпечують прозорість і захищеність обміну інформацією; а також створення захищених цифрових платформ, що використовують алгоритми штучного інтелекту для моніторингу аномальної активності, виявлення потенційних кібератак і автоматизованої реакції на інциденти [49, 100, 104]. Такі технології відкривають нові можливості для підвищення рівня кіберзахисту, але водночас вимагають адаптації існуючих нормативних актів, а також значних фінансових вкладень у технічну модернізацію державних IT-інфраструктур.

У цьому контексті Дереко В. звертає увагу на те, що хоча інноваційні технології дозволяють суттєво підвищити загальний рівень безпеки державних інформаційних систем, їх впровадження супроводжується низкою викликів

[9]. Насамперед, це необхідність значних інвестицій, як фінансових, так і кадрових. Крім того, застосування новітніх рішень вимагає постійного оновлення нормативно-технічної бази, яка повинна відповідати динаміці розвитку цифрових технологій та адаптуватися до нових загроз і викликів у сфері кібербезпеки [9].

Ще однією визначальною характеристикою сучасного підходу до інформаційної безпеки є необхідність створення ефективного механізму управління ризиками. Як зазначає Домбровська С., в умовах цифрової трансформації державного управління критично важливим є регулярне проведення оцінки інформаційних ризиків, безперервний моніторинг стану захищеності інформаційних систем, а також оперативне реагування на інциденти. Такий підхід дозволяє виявити вразливі місця ще до виникнення загрози, а у разі її реалізації - швидко нейтралізувати наслідки та зберегти функціонування цифрових послуг [11].

У цьому ж напрямі деякі дослідники рекомендують впровадження міжнародних стандартів, зокрема NIST Special Publication 800-53A, який розроблений Національним інститутом стандартів і технологій США [100]. Цей документ містить детальні інструкції, алгоритми та шаблони для оцінки ефективності заходів безпеки, що застосовуються в державних інформаційних системах. Він дозволяє уніфікувати процедури контролю, забезпечити прозорість дій та адаптувати безпекову політику до вимог конкретного середовища, в якому функціонує система [100].

Наступною особливістю є нормативно-правове забезпечення інформаційної безпеки. Як зазначає Нашинець-Наумова А., для створення ефективної системи інформаційної безпеки необхідне чітке законодавче регулювання, яке б відповідало сучасним викликам і міжнародним стандартам. Це передбачає не лише прийняття відповідних нормативно-правових актів, а й активну участь держави у формуванні міжнародних стандартів та укладення міжнародних угод з інформаційної безпеки [49].

З огляду на швидкі темпи цифровізації управлінських процесів, особливе значення набуває підвищення інформаційної культури державних службовців і громадян. Харченко Л., Ліпкан В. та Логінов О. наголошують, що забезпечення інформаційної безпеки неможливе без активного впровадження освітніх програм, які спрямовані на підвищення обізнаності користувачів щодо кіберзагроз та правил безпечного поводження з інформацією [68].

Також важливою особливістю є залучення громадянського суспільства та приватного сектору до процесів забезпечення інформаційної безпеки, необхідності широкої кооперації державних органів, бізнесу та громадськості для створення ефективної екосистеми безпеки цифрових державних послуг [104]. Забезпечення інформаційної безпеки в умовах цифровізації державного управління вимагає системного, багатовимірного підходу, який передбачає впровадження новітніх технологій, розвиток нормативно-правового регулювання, підвищення рівня інформаційної культури суспільства, а також тісну взаємодію між державою, бізнесом та громадськістю для своєчасного реагування на сучасні інформаційні загрози.

У процесі формування ефективної системи інформаційної безпеки в умовах електронного урядування особливого значення набуває детальна класифікація інформаційних загроз [44]. Така класифікація дозволяє не лише виявляти джерела потенційних загроз, але й формувати відповідні стратегії управління ризиками, що забезпечують надійність функціонування цифрової державної інфраструктури. Розглянемо більш детально класифікацію.

1. Класифікація за походженням. У контексті електронного урядування інформаційні загрози за походженням поділяються на внутрішні та зовнішні. Такий поділ є надзвичайно важливим для побудови системи багаторівневого захисту державних цифрових платформ та інформаційних систем.

1.1. Внутрішні загрози формуються безпосередньо всередині органів державної влади або в межах інформаційної системи, якою вони користуються. Основними джерелами внутрішніх загроз виступають помилки персоналу внаслідок недостатнього рівня цифрової грамотності або

неналежної підготовки; порушення регламентів доступу до інформації; недотримання правил зберігання та обробки даних; службова недбалість або навмисні деструктивні дії з боку співробітників; технічні дефекти у роботі інформаційних систем, пов’язані з проєктувальними помилками або моральним зношенням інфраструктури [4, 10, 44]. У межах електронного урядування внутрішні загрози можуть проявлятися у вигляді помилок під час адміністрування електронних реєстрів, неправомірної модифікації даних у системах документообігу, або ненавмисного розголошення персональної інформації громадян.

1.2. Зовнішні загрози мають своє джерело поза межами державної інформаційної системи, здебільшого є цілеспрямованими та системними. До найбільш поширених зовнішніх загроз належать хакерські атаки, спрямовані на виведення з ладу державних онлайн-платформ; зловмисне програмне забезпечення, що вводиться у систему з метою шпигунства або шантажу; діяльність іноземних спецслужб, спрямована на дестабілізацію цифрової інфраструктури держави; кіберзлочинність, орієнтована на крадіжку персональних даних або фінансову вигоду; стихійні лиха або техногенні катастрофи, які призводять до знищення або пошкодження фізичних носіїв інформації, серверів чи центрів обробки даних [9, 11, 30]. В електронному урядуванні зовнішні загрози можуть, наприклад, спричинити тимчасову недоступність державних сервісів, що унеможливлює безперервне надання послуг громадянам і бізнесу.

2. Класифікація за характером дії. За характером впливу на інформаційні системи загрози відображають спосіб реалізації загроз і рівень їх деструктивного потенціалу.

2.1. Пасивні загрози передбачають несанкціоноване спостереження за передачею або зберіганням інформації без прямого втручання в її структуру чи зміст [9]. Такі загрози зазвичай залишаються непоміченими, однак можуть становити серйозну небезпеку з точки зору порушення конфіденційності. У межах електронного урядування прикладом пасивних загроз може бути

перехоплення зашифрованого трафіку між інформаційною системою органу влади та зовнішніми сервісами, а також зчитування даних із незахищених електронних реєстрів.

2.2. Активні загрози, на відміну від пасивних, пов’язані з прямим впливом на функціонування інформаційних систем [74]. Вони мають на меті порушити цілісність, доступність або автентичність інформації. До активних загроз можна віднести впровадження вірусів і шкідливого коду в інформаційні системи органів влади; атаки типу «відмова в обслуговуванні», що блокують доступ до цифрових послуг; спроби модифікації або знищення офіційних електронних документів; несанкціоноване втручання в системи голосування або адміністрування державних реєстрів [9, 49, 74].

3. Класифікація за наслідками. Ще одним важливим підходом до класифікації є аналіз потенційних наслідків, які викликає реалізація інформаційних загроз. Цей критерій є ключовим у побудові системи управління інформаційними ризиками.

3.1. Загрози конфіденційності пов’язані з можливістю витоку, розголошення або несанкціонованого доступу до персональних або службових даних [68]. У сфері електронного урядування це може включати отримання зловмисником відомостей із державних баз даних.

3.2. Загрози цілісності виникають у випадках спотворення або фальсифікації даних. Така ситуація є вкрай небезпечною в державному секторі, оскільки призводить до прийняття хибних управлінських рішень, а також підриває легітимність електронного документообігу.

3.3. Загрози доступності стосуються недоступності або збоїв у роботі інформаційних систем. Це може бути наслідком атак, збоїв у живленні, відмови серверів або втрати інтернет-зв’язку. Така ситуація особливо критична для порталів електронного уряду, які забезпечують надання адміністративних послуг у режимі онлайн [4].

3.4. Загрози автентичності пов’язані з підміною або фальсифікацією цифрових ідентифікаторів, підписів або електронних документів. Це ставить

під сумнів справжність інформації, що циркулює в системі, і може бути використане для шахрайства або дезінформації [4, 68, 74].

Інформаційні загрози в системі електронного урядування мають широкий спектр негативних наслідків, що можуть істотно вплинути на стабільність державного управління та загальну безпеку держави. Найперше, втрата конфіденційності інформації є серйозною загрозою, оскільки вона передбачає можливість витоку або несанкціонованого поширення персональних та державних даних. Це, своєю чергою, призводить до зниження рівня довіри громадян до державних органів, втрати авторитету влади і формування негативних суспільних настроїв [49, 100]. Витік персональних даних може спричинити значні порушення прав і свобод громадян, включаючи загрозу їх фінансовій та соціальній безпеці, що підриває основи демократичного суспільства [49]. Крім того, використання таких даних зловмисниками може призводити до шахрайства, шантажу, фінансових злочинів та інших серйозних правопорушень [100].

Наступною істотною проблемою є порушення цілісності інформації. Цей аспект має безпосередній вплив на процес ухвалення державних рішень, оскільки достовірність і точність інформації є вирішальними чинниками для прийняття ефективних управлінських рішень. Фальсифікація або викривлення інформації може призводити до помилкових висновків і неадекватних рішень, які можуть мати серйозні економічні, політичні та соціальні наслідки [9]. Зокрема, рішення, прийняті на основі недостовірних даних, можуть спричиняти неефективне використання бюджетних ресурсів, підрив економічної стабільності та зниження конкурентоспроможності держави на міжнародній арені [4, 104].

Не менш важливим є забезпечення доступності інформації, оскільки будь-які перебої у функціонуванні державних електронних сервісів або інформаційних систем можуть мати руйнівні наслідки для повсякденного життя громадян, діяльності бізнесу та функціонування державних інституцій. Втрата доступності може бути викликана такими загрозами, як кібератаки

(наприклад, DDoS-атаки), вірусні атаки або збої технічного характеру [30, 32]. Подібні ситуації здатні паралізувати функціонування критичних інфраструктур, зокрема медичних, фінансових, транспортних і соціальних сервісів, що створює серйозні кризові умови в суспільстві. За таких умов органи влади втрачають здатність оперативно реагувати на потреби населення, що підриває не лише стабільність, а й авторитет влади в очах громадян [32].

Крім того, порушення доступності інформації та електронних послуг має негативний вплив і на міжнародний імідж держави. Держава, яка не здатна забезпечити надійність своїх цифрових систем, сприймається як менш стабільний та надійний партнер у міжнародних відносинах. Це може призводити до втрати інвестицій, ускладнення дипломатичних стосунків, а також до зниження конкурентоспроможності країни на міжнародному рівні [30]. Тому ефективне управління інформаційними ризиками має стати пріоритетним завданням державної політики, що передбачає розробку комплексних заходів з інформаційної безпеки, постійне навчання персоналу і розвиток сучасних технологічних рішень [4, 49, 9, 100, 104].

Викладені у пп.1.1 і 1.2 результати проведених дослідженнь дозволили сформувати цілісне уявлення про теоретичну сутність електронного урядування як складної системи, що функціонує в умовах цифрової трансформації публічного сектору. Ідентифіковано, що ефективність цифрової взаємодії між державою, громадянами та бізнесом безпосередньо залежить від здатності держави забезпечити надійний захист інформаційних ресурсів та інфраструктури. З урахуванням наукових підходів, класифікацій загроз, а також особливостей правового, технічного та організаційного захисту, виявлено, що інформаційна безпека повинна бути системно інтегрована в архітектуру електронного урядування. Відповідна системна модель представлена на рисунку 1.5 і є підґрунтям для подальшого аналізу організаційно-управлінських механізмів інформаційної безпеки у наступних розділах дослідження.

Рисунок 1.5. Системна модель взаємозв'язку між електронним урядуванням, його завданнями, функціями, інформаційною безпекою та загрозами

Джерело: розроблено автором

Наведена модель дозволяє розглядати електронне урядування як багатокомпонентну систему, в якій завдання та функції управління реалізуються через цифрові інструменти, що, у свою чергу, формують інтенсивні інформаційні потоки між державними органами, громадянами та бізнесом. Саме ці потоки стають об'єктами як розвитку, так і потенційних ризиків. Модель також демонструє, що інформаційна безпека виступає не окремим функціональним блоком, а наскрізною категорією, яка інтегрується у всі рівні функціонування електронного урядування від правового забезпечення до технічного й організаційного рівнів. Загрози інформаційній безпеці, зображені як зовнішні та внутрішні чинники, вказують на необхідність системної реакції державного управління на виклики цифрового середовища. Відповідно, забезпечення стійкості та стабільності системи електронного урядування потребує системного підходу, що поєднує інституційні, правові, технічні й освітні заходи.

Системний підхід до інформаційної безпеки є запорукою стабільності державного управління в умовах цифровізації та основою для подальшого розвитку електронного урядування. Водночас, глобальні виклики інформаційної безпеки, стрімкий розвиток технологій та зростання кількості кібератак обумовлюють необхідність звернення до міжнародного досвіду. Саме міжнародна практика забезпечення інформаційної безпеки в електронному урядуванні дозволяє ідентифікувати ефективні підходи, стандарти та інструменти, які можуть бути адаптовані в Україні з урахуванням національних соціо-економічних і геополітичних особливостей.

1.3. Міжнародний досвід забезпечення інформаційної безпеки в електронному урядуванні

Міжнародний досвід розвитку електронного урядування демонструє сталі позитивні тенденції, що супроводжуються поглибленням цифровізації публічного сектору, підвищенням доступності електронних послуг та

активним впровадженням новітніх інформаційно-комунікаційних технологій. Відповідно до UN E-Government Survey 2024, середнє глобальне значення Індексу розвитку електронного урядування (EGDI) становило 0,6382 [114], що свідчить про поступове зміцнення цифрового потенціалу державного управління у більшості країн світу. Для порівняння, у 2022 році середнє значення EGDI дорівнювало 0,6102 [114]. Країнами-лідерами в рейтингу EGDI стали Данія, Естонія та Сінгапур (рис.1.6), які демонструють високий рівень інтегрованих електронних послуг, надійну інформаційно-комунікаційну інфраструктуру, а також ефективні інституційні механізми забезпечення кібербезпеки та цифрової довіри.

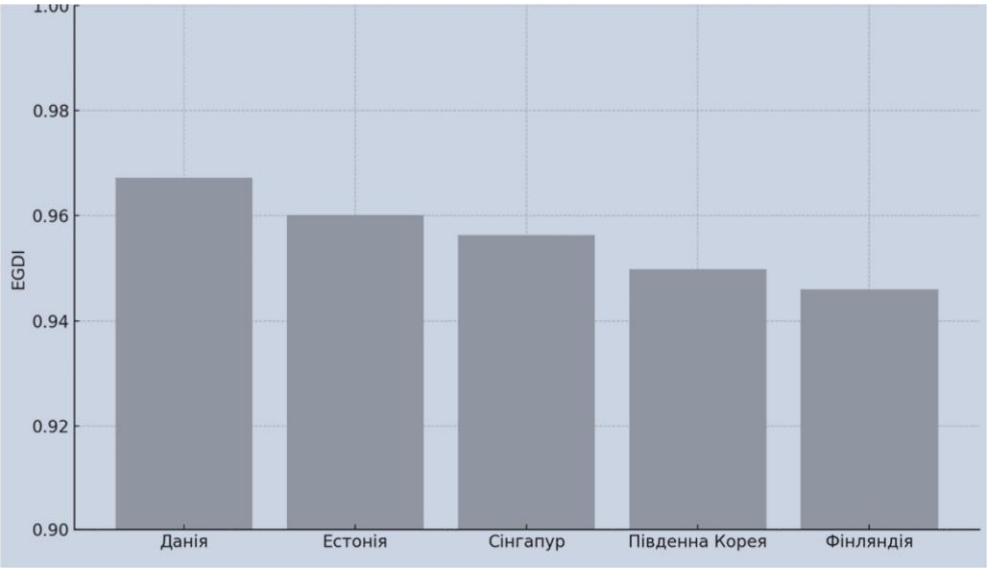


Рисунок 1.6 . Країни-лідери за Індексом розвитку електронного урядування у 2024 році

Джерело: побудовано автором на основі UN E-Government Survey 2024 [114]

Наприклад, Естонія реалізує концепцію «держави як платформи», в якій кожна державна послуга доступна онлайн, а захист персональних даних здійснюється на основі технології блокчейн. Натомість, Данія активно впроваджує цифрову ідентичність та європейські стандарти інформаційної безпеки, зокрема в частині управління ризиками та відповідальності держави за цифрову інфраструктуру [114].

У регіональному розрізі Європа зберігає лідерські позиції - 84% країн мають високі значення EGDI (рис.1.7). У країнах Азії цей показник становить 53%, в Америці - 57%, тоді як в Африці та Океанії - відповідно 52% та 57% демонструють середній рівень розвитку електронного урядування [114].

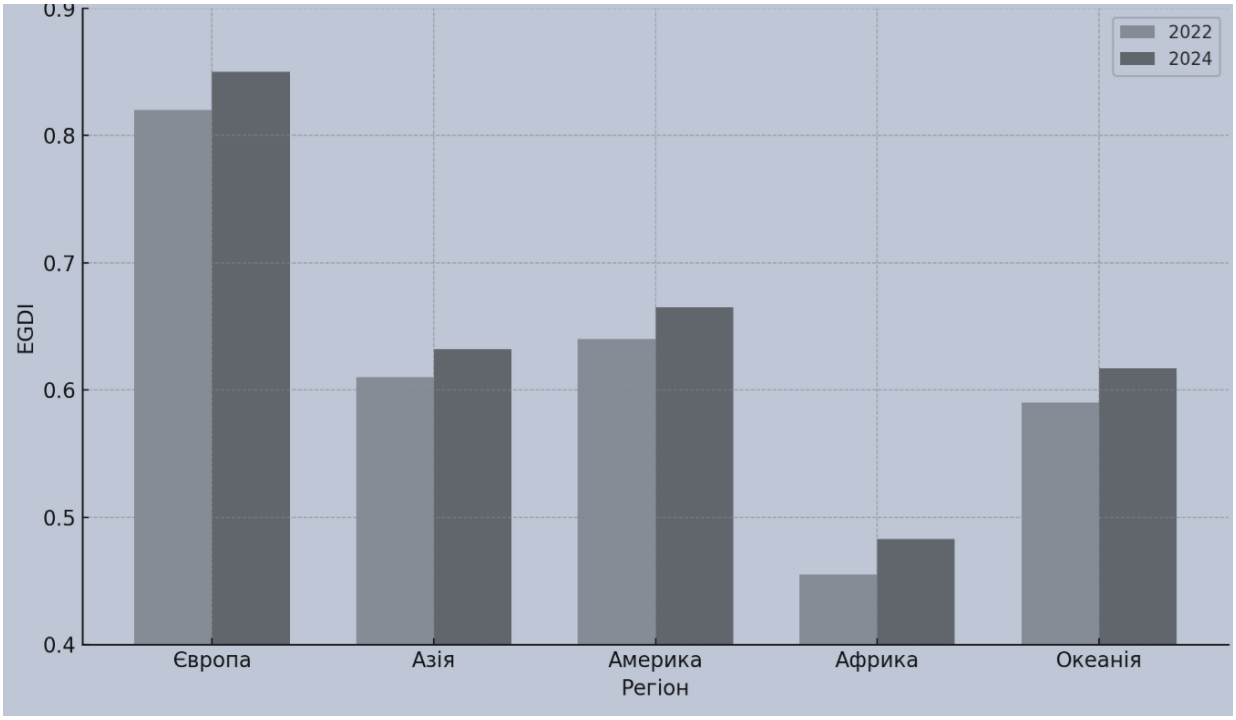


Рисунок 1.7. Порівняння Індексу розвитку електронного урядування (EGDI) за регіонами у 2022 та 2024 роках

Джерело: побудовано автором за даними UN E-Government Survey 2024 [114]

У країнах із середнім і низьким рівнем доходу спостерігається прогрес у сфері цифровізації базових адміністративних процедур, однак саме ці держави залишаються найбільш вразливими до зовнішніх інформаційних загроз, зокрема кібератак та порушень захисту персональних даних.

Паралельно з розвитком електронного врядування, в міжнародній практиці посилюється акцент на питаннях забезпечення інформаційної безпеки як ключового елементу цифрової стійкості держави. Це пов’язано з тим, що розширення обсягів обробки чутливої інформації та перенесення управлінських процесів у цифрове середовище підвищують рівень ризиків,

пов’язаних з кіберінцидентами. Як зазначено у доповіді Human Development Report 2023-2024, сучасний світ перебуває у стані глобального технологічного протистояння, що посилює поляризацію у сфері цифрових можливостей, створюючи виклики для міжнародної співпраці в галузі кібербезпеки [109].

Проблеми забезпечення інформаційної безпеки також фіксуються у світовій аналітиці щодо стану цифрових державних платформ. Згідно з аналітичним оглядом, проведеним у 2023 році [104], на основі оцінки понад 3000 офіційних урядових сайтів, у багатьох країнах державні платформи не відповідають навіть базовим міжнародним стандартам безпеки (зокрема TLS 1.2+ шифрування, DNSSEC, SPF/DKIM для захисту e-mail тощо) [104]. У цьому контексті особливо актуальним є питання впровадження комплексних політик інформаційної безпеки, що включають постійний моніторинг вразливостей, інституційне управління ризиками, розбудову інфраструктури кіберзахисту та створення національних команд реагування на інциденти безпеки.

Ряд країн, зокрема Канада, Південна Корея, Нідерланди та Ізраїль, демонструють ефективні моделі інформаційної безпеки в системі електронного урядування. Так, у Канаді впроваджено CyberSecure Canada - програму сертифікації, що вимагає від державних і приватних суб’єктів дотримання визначених вимог до інформаційної безпеки, включаючи шифрування, резервне копіювання, політики оновлення ПЗ тощо. В Ізраїлі функціонує Національний центр кібербезпеки, який координує взаємодію урядових структур, бізнесу та наукової спільноти у сфері реагування на кіберзагрози.

Узагальнюючи зазначене, слід констатувати, що міжнародна практика забезпечення інформаційної безпеки в системах електронного урядування базується на таких ключових засадах як:

- розробка національних стратегій кібербезпеки;
- інтеграція міжнародних стандартів ISO/IEC 27001 та NIST SP 800-53 у державне управління;

- міжвідомча та міждержавна координація дій у сфері цифрової безпеки;
- постійне підвищення цифрової грамотності користувачів та державних службовців;
- розвиток інфраструктури національного моніторингу й реагування на загрози.

Сучасна динаміка розвитку електронного урядування все більшою мірою пов’язується з упровадженням інструментів штучного інтелекту (ШІ), які істотно змінюють не лише механізми надання державних послуг, але й загальну парадигму публічного управління. У глобальних звітах ООН наголошується на тому, що застосування ШІ переходить від етапу експериментального тестування до етапу системної інтеграції у ключові управлінські процеси [111, 104, 109, 114]. Це зумовлює необхідність переосмислення функцій держави в умовах цифрової взаємодії.

Згідно з даними UN E-Government Survey 2024, на початку 2020-х років лідерами у впровадженні ШІ в електронне урядування стали Сінгапур, Естонія, Данія, Південна Корея та Фінляндія [114]. Ці країни не лише очолюють рейтинг EGDI, але й демонструють найвищій ступінь готовності до використання штучного інтелекту в державному управлінні. Сінгапур активно застосовує системи прогнозного аналізу для оптимізації мобільності, медичних сервісів та соціального захисту. Уряд використовує ШІ як платформу для прийняття оперативних рішень на основі даних у реальному часі. В Естонії ШІ впроваджено в інфраструктуру «невидимого уряду», де адміністративні послуги автоматизовано до такого ступеня, що взаємодія громадян з державою відбувається майже без людського втручання [114].

У свою чергу, Данія зосередилася на створенні етичних засад використання штучного інтелекту в публічному управлінні, впроваджуючи обов’язкові національні стандарти прозорості алгоритмів. Подібний підхід також реалізується у Фінляндії, де крім технічних інструментів, значну увагу

приділяють цифровій освіті громадян і державних службовців у контексті роботи з алгоритмічними системами.

У доповіді Human Development Report 2023-2024 акцентується увага на тому, що саме інтеграція ШІ в державне управління має потенціал компенсувати кризу ефективності та довіри до традиційних інституцій [109]. Автори документа підкреслюють, що у країнах з високим індексом людського розвитку та високим EGDI спостерігається позитивна кореляція між рівнем впровадження інтелектуальних державних сервісів і задоволеністю громадян якістю управлінських рішень. Більш того, цифрові уряди, які застосовують ШІ у процесах комунікації, виявлення потреб населення, управління кризами та розподілу ресурсів, демонструють кращі показники соціальної згуртованості та демократичної участі.

Водночас, глобальні звіти відзначають глибоку асиметрію в рівні інтеграції ШІ у державне управління по різних країнах і регіонах. Якщо у високорозвинених країнах ШІ вже виконує функції підтримки прийняття рішень у реальному часі, то в країнах із середнім та низьким рівнем доходу ШІ або не впроваджений, або застосовується в пілотних масштабах, головним чином у сферах охорони здоров’я чи електронної ідентифікації. Це створює ризики поглиблення цифрового розриву між державами та підвищує залежність менш розвинених країн від зовнішніх постачальників алгоритмічних рішень, що загрожує зниженням суверенітету у сфері управління інформацією.

Крім технічних питань, значна увага приділяється нормативним та етичним аспектам застосування ШІ. Прозорість алгоритмів, недискримінаційність цифрових сервісів, а також питання приватності громадян в умовах обробки великих обсягів персональних даних - усе це формує нові вимоги до цифрової політики урядів. Як зазначається, майбутнє ефективного електронного урядування не стільки в обсягах технологічного впровадження, скільки у здатності держав гармонізувати розвиток ШІ з принципами демократії, підзвітності та відкритості. Країни, що демонструють

успішні приклади впровадження ШІ, орієнтуються не лише на технічну ефективність, а й на соціальну адаптивність та довіру громадян. Такий підхід дозволяє формувати цифрову державу, спроможну відповідати на виклики сучасного глобалізованого світу та водночас зберігати гуманітарну цінність публічного управління.

Активізація використання технологій штучного інтелекту в системах електронного урядування, поряд із розширенням потенціалу управлінських рішень, водночас загострює питання забезпечення інформаційної безпеки як ключового елементу цифрової стійкості держави. Міжнародний досвід свідчить про формування нових підходів до регулювання ШІ, у межах яких безпековий компонент стає вирішальним фактором цифрової політики (табл.1.3).

Таблиця 1.3. Ініціативи у регулюванні ШІ в контексті інформаційної безпеки

Країна / Регіональні об'єднання	Ключові документи / ініціативи	Основний акцент
Європейський Союз	AI Act, DSA, DMA, GDPR	Регуляція за рівнем ризику, інтеграція з GDPR
США	Executive Order 14110, NIST AI RMF	Добровільні стандарти, міжвідомчий підхід
Велика Британія	White Paper on AI, AI Regulation Bill (draft)	Гнучкість, стимулювання інновацій
Китай	Algorithm Regulation, GenAI Measures, Global AI Governance Initiative	Централізований контроль, відповідність державним стандартам
Канада	AIDA (Bill C-27)	Прозорість і відповідальність у прийнятті рішень
Бразилія	EBIA, AI Regulatory Bill (draft)	Баланс інновацій і етики
Сінгапур	AI Governance Framework, AI Verify	Етичність, довіра та прозорість ШІ
Південна Корея	AI Industry Promotion and Trust Act	Сприяння індустрії ШІ та формування довіри
OECD	OECD AI Principles	Міжнародні стандарти відповідального ШІ

Джерело: систематизовано і побудовано автором на основі [75]

У межах Європейського Союзу, наприклад, система нормативного забезпечення безпеки використання ШІ включає не лише технологічні вимоги, а й елементи правової відповідальності за порушення інформаційних прав громадян. Запроваджуваний AI Act, тісно інтегрований з Регламентом захисту персональних даних (GDPR), закріплює ризик-орієнтований підхід, згідно з яким системи високого ризику, зокрема ті, що функціонують у публічному секторі, підлягають ретельній оцінці та сертифікації. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу до критичних даних, маніпуляції результатами обробки інформації та порушення принципів прозорості алгоритмічних рішень.

У Сполучених Штатах Америки, з урахуванням децентралізованої моделі управління, пріоритет у сфері безпеки ШІ надається розробці добровільних стандартів на рівні інституцій. Документ NIST AI Risk Management Framework пропонує універсальні принципи оцінки ризиків, включаючи кіберзагрози, а також інструменти для зменшення вразливостей у системах, що працюють з персональними та службовими даними. Виконавчий наказ №14110, підписаний у 2023 році, підкреслює важливість міжвідомчої координації для створення безпечного цифрового середовища в державному секторі, з урахуванням зростаючих викликів кібербезпеки.

У Великій Британії, яка прагне зберегти баланс між інноваціями та захистом інформації, розробляється проект закону про ШІ, що передбачає створення адаптивної регуляторної рамки. Білий документ уряду («Pro-Innovation Approach to AI Regulation») містить положення про забезпечення надійності даних та обов’язкової ідентифікації джерел алгоритмічних рішень. Тобто, у політиці Великої Британії безпека цифрових рішень розглядається як передумова довіри до інтелектуальних сервісів публічного управління. Запроваджено Data Ethics Framework, який регламентує прозорість алгоритмів, які використовуються в електронному врядуванні [42, 79].

Особливої уваги заслуговує підхід Китаю, де інформаційна безпека є базовою складовою державного регулювання цифрових технологій. Через прийняття Положення про управління генеративним ШІ та Алгоритмічного управління онлайн-платформами, держава встановлює жорсткий контроль над потоками інформації, алгоритмами обробки даних та оцінкою контенту, що генерується ШІ. Така модель характеризується пріоритетом державного суверенітету над інформаційним простором і повною відповідальністю за кіберзахист у публічному секторі.

У країнах Азії, зокрема в Сінгапурі, впроваджено моделі добровільної сертифікації безпеки штучного інтелекту, зокрема платформу AI Verify, що дозволяє бізнесу та державним органам оцінювати відповідність ШІ-систем критеріям прозорості, справедливості, безпеки та надійності. Важливим елементом є наявність етичної рамки управління, яка забезпечує не лише технічну безпеку, а й соціальну довіру до державних цифрових сервісів [79]. Цей підхід заснований на презумпції довіри до цифрових сервісів лише за умови дотримання критеріїв інформаційної безпеки, що відповідає підходу «security-by-design».

Ефективне функціонування електронного урядування неможливе без належного рівня інформаційної безпеки. Світові практики демонструють широкий спектр моделей, механізмів і інструментів, спрямованих на забезпечення захисту інформаційних ресурсів держави, особливо в контексті впровадження інноваційних технологій у публічне управління.

Одним із найбільш інноваційних прикладів є Естонія, де сформована унікальна модель цифрового суверенітету. Інформаційна безпека забезпечується через інтеграцію технологій блокчейн (KSI), національної платформи X-Road, а також електронної ідентифікації (e-ID). Ця країна першою у світі запровадила концепцію «електронного резидентства», що передбачає безпечний транскордонний доступ до державних послуг. Враховуючи високий рівень автоматизації, питання захисту даних громадян і

прозорості управління знаходяться в центрі політики національної безпеки [5, 46].

Фінляндія впровадила модель централізованого зберігання державних даних із жорсткими протоколами доступу. Національна цифрова інфраструктура включає сервіси Kanta та Suomi.fi, які гарантують захищений обмін інформацією між громадянами, медичними установами, органами державної влади. Впровадження цифрових паспортів і безпечних ідентифікаційних систем дозволяє країні досягати високого рівня стійкості до кіберзагроз та гарантувати конфіденційність персональних даних [27].

Канада дотримується моделі «відкритого уряду"» в якій інформаційна безпека балансується з прозорістю та публічністю. Основними регуляторами є Digital Charter та Privacy by Design, що передбачають вбудовану у дизайн цифрових сервісів приватність та відповідність правам громадян на інформаційний захист [41, 79]. Цей підхід демонструє, як безпека може не обмежувати доступ, а підсилювати його легітимність.

У порівняльному аспекті можна виокремити кілька підходів до забезпечення інформаційної безпеки в електронному урядуванні (табл.1.4).

Таблиця 1.4. Порівняльна характеристика підходів до забезпечення інформаційної безпеки в електронному урядуванні

Країна	Модель безпеки	Ключові інструменти	Підхід до регулювання
Естонія	Цифровий суверенітет, блокчейн-захист, міжвідомча інтеграція	e-ID, KSI, X-Road, e-Residency	Інституційний і технологічний
Фінляндія	Централізовані державні сервіси з підвищеною кібербезпекою	Kanta Services, Suomi.fi, цифрові паспорти	Централізовано-інфраструктурний
США	Федеральна модель з акцентом на стандарти (NIST, FISMA)	NIST RMF, Cybersecurity Act, Executive Order 14110	Децентралізовано-нормативний
Канада	Вбудований захист приватності, відкритий уряд	Digital Charter, Privacy by Design, Data Act	Принцип приватності за замовчуванням
Сінгапур	Сертифікація надійності ШІ-систем, етична відповідність	AI Verify, AI Governance Framework	Добровільна етична сертифікація
Велика Британія	Гнучка нормативна модель, нагляд за етикою ШІ	White Paper on AI, Data Ethics Framework	Право, етика і гнучкість
Південна Корея	Державна програма цифрової довіри, етичний ШІ-закон	AI Industry Promotion Law, цифрові ID, блокчейн	Державне регулювання і суспільна довіра
Німеччина	Технічний контроль і правові рамки кіберзахисту	BSI Grundschutz, eGovernment Act	Національні технічні стандарти
Франція	Національна стратегія цифрової безпеки та ШІ-сертифікація	CNIL, SREN Law, план кібернагляду	Законодавча і наглядова модель
Китай	Централізоване кіберрегулювання, контроль алгоритмів	Алгоритмічне регулювання, ГенAI-закон	Централізовано-регламентований
Японія	Система цифрової ідентифікації та кіберспроможності	My Number, e-Residency Japan, MIC Guidelines	Техно-адміністративний
Австралія	Модель кіберстійкості на базі національного центру	Australian Cyber Security Strategy, GovPass	Гібридний (нормативно-інституційний)

Джерело: систематизовано і побудовано автором на основі [7, 42, 46, 87, 109, 117, 120]

Усі ці підходи об’єднує спільна мета - сформувати стійку інфраструктуру державного управління, де захист даних, безпека комунікацій та довіра громадян є ключовими критеріями ефективності електронного врядування. Відповідно, ключовими факторами успішного забезпечення інформаційної безпеки можна ідентифікувати [7, 46, 79]:

- наявність стратегії кібербезпеки, узгодженої з політикою електронного урядування;
- законодавче забезпечення захисту персональних даних;
- підвищення рівня цифрової грамотності державних службовців;
- розвиток державно-приватного партнерства в сфері безпеки цифрових послуг.

Сучасна трансформація суспільних відносин та моделей управління державою є об’єктивною необхідністю. Йдеться про докорінну зміну філософії державного управління, в якій домінують принципи інноваційності, відкритості, орієнтації на потреби громадян та забезпечення комплексної інформаційної безпеки. Реалізація цифрового уряду забезпечує переорієнтацію державних інституцій на потреби громадян, підвищення ефективності адміністративних процесів та розширення демократичної участі. Впровадження цифрового уряду вже демонструє високі результати у таких країнах, як Естонія, Фінляндія, Південна Корея, Сінгапур, Канада, Велика Британія, Австралія, Данія та Японія, які успішно реалізують комплексні цифрові стратегії, поєднуючи цифровізацію державних послуг із забезпеченням інформаційної безпеки, етики штучного інтелекту та участі громадян. Більшість з цих країн стабільно входять до верхніх позицій Індексу розвитку електронного урядування ООН (EGDI) [114], що свідчить про ефективність їхніх підходів до цифрової трансформації публічного сектору.

У звіті ООН «UN E-Government Survey 2024» цифровий уряд трактується як «екосистема взаємопов’язаних інституцій, процесів і технологій, що функціонують у цифровому середовищі, керуючись принципами орієнтації на користувача, інклюзивності, довіри та безпеки» [114].

Рисунок 1.8. Теоретичний конструкт цифрового уряду

Джерело: розроблено автором

Такий підхід передбачає не лише функціональну модернізацію державного апарату, а й створення цифрового простору, в якому відбувається безперервна взаємодія між органами влади, громадянами, бізнесом і громадським сектором. Цифровий уряд втілює ідею багаторівневої співпраці в умовах прозорості, інтероперабельності систем і активного використання передових технологій (рис.1.8).

На відміну від класичного електронного урядування, яке концентрувалося переважно на наданні доступу до публічних сервісів через цифрові канали, концепція цифрового уряду базується на екосистемному підході. Його суть полягає у побудові відкритої цифрової платформи, що забезпечує взаємозв'язок та інтеграцію між усіма зацікавленими сторонами - державними інституціями, громадянами, науковими установами, підприємствами й міжнародними партнерами. Така модель передбачає оперативне ухвалення управлінських рішень, персоніфікацію державних послуг, широке залучення населення до політичного процесу та використання інноваційних технологій, включаючи штучний інтелект, великі дані, хмарні обчислення і блокчейн [104, 114].

Крім технічного та організаційного виміру, цифровий уряд має вагоме соціально-політичне значення. Як зазначається у Human Development Report 2023-2024, цифровий уряд розглядається як один із ключових інструментів досягнення суспільної згуртованості, подолання глобальної поляризації та підвищення якості публічного управління [109]. У звіті наголошується, що наявність розвиненої цифрової інфраструктури, спроможність держави забезпечити кібербезпеку та довіру до державних сервісів є визначальними критеріями інституційної стійкості сучасних країн. Особливий акцент робиться на забезпеченні інклюзивного доступу до державних послуг, що дозволяє зменшити соціальні розриви між різними категоріями громадян, зокрема вразливими та маргіналізованими групами.

Цифровий уряд також розглядається як механізм реалізації Цілей сталого розвитку. Його впровадження сприяє досягненню SDG 16 - «Мир,

справедливість та ефективні інститути», оскільки забезпечує прозорість і підзвітність діяльності державних органів. Крім того, цифровий уряд безпосередньо сприяє реалізації SDG 9 - «Інфраструктура, індустріалізація та інновації» через розвиток цифрової інфраструктури та модернізацію управлінських процесів. У контексті міжнародного співробітництва, SDG 17 - «Партнерство заради сталого розвитку» реалізується через електронну дипломатію, транскордонний обмін даними, електронне резидентство та інтегровані послуги [114]. Отже, цифровий уряд є не лише наступним етапом еволюції електронного урядування, але й концептуальним вектором розвитку публічного управління, зорієнтованого на сталий розвиток, цифрову інклюзію, технологічну адаптивність та безпечне функціонування у цифровому середовищі. Його реалізація вимагає комплексного міждисциплінарного підходу, що включає правові, організаційні, технічні й соціальні інструменти, а також високий рівень цифрової культури як з боку держави, так і громадянського суспільства.

Аналіз міжнародного досвіду функціонування систем електронного та цифрового урядування дозволив виокремити ключові елементи ефективного забезпечення інформаційної безпеки в умовах цифрової трансформації публічного управління. Досвід таких країн, як Естонія, Сінгапур, Південна Корея, Канада, Данія, Швеція та Великобританія, свідчить про те, що інформаційна безпека не може бути розглянута як окремий технічний елемент, а має інтегруватися у всі рівні електронного урядування як його невід’ємна складова [104, 109, 114].

Для України цей досвід є важливим, оскільки дозволяє окреслити реалістичні та обґрунтовані напрями вдосконалення національної моделі електронного урядування з урахуванням вимог кібербезпеки, цифрових прав громадян та новітніх технологій. Ефективна імплементація міжнародних підходів до розвитку електронного урядування та забезпечення інформаційної безпеки має базуватися на низці ключових стратегічних напрямів, які

враховують як зарубіжні практики, так і національні виклики. Серед них варто виокремити:

1. Розробку та затвердження Національної стратегії цифрового урядування України, яка має містити системне бачення розвитку цифрових державних інституцій. У рамках цієї стратегії необхідно визначити інформаційну безпеку не як допоміжну функцію, а як інтегральну складову всіх етапів життєвого циклу цифрових сервісів - від планування, дизайну, реалізації до оцінювання ефективності. Важливо, щоб безпека закладалася на рівні архітектури цифрових платформ, стандартів інтероперабельності, політик захисту даних та управління доступом.

2. Формування постійно діючої міжвідомчої координаційної структури з питань цифрової безпеки та довіри, за прикладом Естонського агентства інформаційних систем. Такий орган повинен об’єднувати функції стратегічного аналізу загроз, розробки стандартів і політик у сфері інформаційної безпеки, моніторингу цифрової інфраструктури та реагування на інциденти, а також забезпечувати міжвідомчу координацію між секторами влади, бізнесом та громадянським суспільством.

3. Гармонізацію нормативно-правової бази з міжнародними стандартами, зокрема стандартами кіберзахисту, рекомендаціями ООН і ЄС. Це дозволить забезпечити належний рівень безпеки обробки персональних та службових даних, а також сприятиме підвищенню довіри до українських цифрових сервісів з боку міжнародних партнерів та користувачів.

4. Впровадження системної цифрової освіти та підвищення кваліфікації для державних службовців, з акцентом на кібергігієну, управління цифровими ризиками, безпечну роботу з даними та розуміння загроз, пов’язаних з використанням новітніх технологій. Крім того, має бути сформована широка програма просвітницької роботи серед громадян щодо їхніх цифрових прав і правил безпечного користування державними е-сервісами, як це реалізується у Сінгапурі, Канаді та Фінляндії.

5. Активне використання інноваційних технологій у сфері інформаційної безпеки, зокрема рішень на основі штучного інтелекту для виявлення аномальної поведінки в системах, технологій блокчейн для забезпечення прозорості транзакцій та збереження цифрових слідів, а також аналізу великих даних для прогнозування кіберзагроз. Україна має врахувати приклади Естонії та Південної Кореї, де подібні інструменти вже є основою державної цифрової інфраструктури.

6. Розбудову механізмів прозорого управління даними, е-участі та громадського контролю, що включає створення відкритих платформ для консультацій, петицій, оцінювання якості послуг, подання скарг і пропозицій. Це дозволить залучити громадян до цифрового врядування, підвищити легітимність рішень і зміцнити довіру до цифрової держави. Відкритість даних має супроводжуватися одночасним дотриманням принципів цифрової етики та безпеки, як це успішно реалізовано у Великобританії через платформу GOV.UK.

Усі ці напрями є не лише практично реалізованими в інших державах, а й можуть бути адаптовані до українських реалій з урахуванням геополітичних викликів, потреб безпеки та прагнення до цифрової інтеграції з ЄС.

Висновки до розділу 1

Проведене теоретичне дослідження електронного урядування в поєднанні з проблематикою інформаційної безпеки дозволяє сформулювати такі узагальнення:

1. З’ясовано, що електронне урядування є багаторівневою системою цифрової взаємодії держави, громадян, бізнесу та громадських організацій, яка охоплює не лише автоматизацію адміністративних процедур, а й трансформацію підходів до управління на засадах відкритості, підзвітності, ефективності та участі. Його еволюція в напрямку цифрового уряду означає перехід від технологічної модернізації до концептуальної перебудови

публічного управління, орієнтованої на дані, користувача, інклюзивність та цифрову довіру.

2. Визначено, що інформаційна безпека є критичною складовою функціонування електронного урядування, без якої неможливо забезпечити довіру громадян до державних цифрових сервісів. Теоретичний аналіз показав, що інформаційна безпека охоплює правові, технічні, організаційні та соціальні механізми, які забезпечують конфіденційність, цілісність та доступність інформації. Розробка системного підходу до інформаційної безпеки дозволяє враховувати специфіку цифрового середовища державного управління, у тому числі виклики, пов'язані з використанням ШІ, великих даних та блокчейн-технологій.

3. Узагальнено міжнародний досвід забезпечення інформаційної безпеки електронного урядування. Провідні країни впроваджують інституційно-інтегровані моделі електронного урядування, в яких управління інформаційною безпекою інтегроване у всі етапи створення цифрових сервісів. Важливими складовими цього досвіду є міжвідомча координація, правове регулювання на основі міжнародних стандартів, цифрова освіта державних службовців, використання сучасних технологій для раннього виявлення загроз і моніторингу кіберінцидентів.

4. Обґрунтовано необхідність адаптації кращих міжнародних практик до національного контексту України. Для цього доцільно розробити національну стратегію цифрового уряду з інтегрованим компонентом інформаційної безпеки, створити постійно діючий міжвідомчий орган із питань цифрової довіри, гармонізувати законодавство із міжнародними рекомендаціями, посилити цифрову освіту держслужбовців та реалізувати підходи громадської участі в захисті цифрового простору.

5. Показано, що цифровий уряд, як наступний етап еволюції електронного урядування, виступає не лише засобом підвищення ефективності державного управління, але й інструментом досягнення Цілей сталого розвитку ООН (зокрема SDG 9, 16, 17). Його реалізація передбачає

одночасне впровадження цифрових технологій та побудову довіри до публічної влади через прозорість, інклюзію та кіберстійкість.

Все вище зазначене створює теоретичне підґрунтя для подальшого аналізу розвитку електронного урядування в Україні в контексті інформаційної безпеки, і дозволяють обґрунтувати напрями імплементації міжнародного досвіду у національну практику.

Основні положення розділу дисертаційної роботивідображені в працях автора [37, 122]

РОЗДІЛ 2
АНАЛІЗ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Оцінка сучасного стану електронного урядування

Методологічною основою дослідження електронного урядування в Україні нами було обрано комплексний підхід, що поєднує кількісні та якісні методи аналізу, відповідні сучасним тенденціям у сфері публічного управління. Ключовим є порівняльно-аналітичний метод, який дозволяє здійснити оцінювання розвитку електронного урядування в Україні шляхом співставлення його показників у різні часові проміжки, а також у міжнародному контексті. Це забезпечує виявлення переваг і недоліків, що є необхідним для формулювання стратегічних рекомендацій.

Основою кількісного аналізу розвитку системи електронного урядування стали міжнародні рейтинги Організації Об'єднаних Націй, зокрема, Індекс розвитку електронного урядування (E-Government Development Index, EGDI) та індекс електронної участі (E-Participation Index, EPI) [111, 114, 112, 113, 110]. EGDI являє собою комплексний показник, сформований на основі середньозваженого значення таких компонентів, як індекс онлайн-послуг (OSI), який оцінює якість і доступність цифрових сервісів; індекс телекомунікаційної інфраструктури (TII), що характеризує рівень розвитку технічної інфраструктури, та індекс людського капіталу (HCI), який відображає рівень цифрових навичок та готовність населення до використання інформаційно-комунікаційних технологій [114]. Доповнюючи EGDI, індекс електронної участі (EPI) визначає рівень залученості громадян до цифрових комунікацій з органами влади та охоплює такі компоненти, як доступність електронної інформації, можливості онлайн-консультацій та механізми прямого залучення громадян до прийняття рішень [114].

Враховуючи, що індекси EGDI та EPI переважно відображають технічний аспект доступності та функціональності електронних послуг, окремо було проведено аналіз нормативно-правових та організаційних засад захисту інформації. Для поглиблення кількісних показників нами було використано також якісний аналіз, що дозволив враховувати особливості національного контексту розвитку електронного урядування, зокрема питання інформаційної безпеки. Базою такого аналізу стали нормативні та стратегічні документи України, серед яких визначальною є «Концепція розвитку електронного урядування в Україні», затверджена розпорядженням Кабінету Міністрів України № 649-р від 20 вересня 2017 року [39]. Цей документ визначає стратегічні пріоритети та конкретні механізми формування ефективної системи електронного урядування, враховуючи питання безпеки інформаційних ресурсів. Це забезпечило цілісність аналізу, доповнивши його важливими аспектами, що визначають ефективність та безпечність електронних взаємодій у державному управлінні.

Важливою частиною якісного аналізу стали результати соціологічних досліджень щодо рівня використання та сприйняття державних електронних послуг громадянами України. Зокрема, використано аналітичний звіт Програми розвитку ООН «Думки і погляди українців щодо державних електронних послуг у 2023 році» [61], що ґрунтується на результатах загальнонаціонального опитування. Цей звіт містить дані, що дозволяють оцінити реальний стан користування електронними сервісами, а також ставлення громадян до них, включаючи аспекти інформаційної безпеки та рівня довіри до державних цифрових платформ. Крім того, враховано результати оцінки Світового банку, викладені у звіті «Ukraine e-Government Assessment» (2018) [118], що надав системний аналіз інституційних, технологічних та нормативних передумов впровадження електронного урядування в Україні.

Становлення і розвиток електронного урядування в Україні відбувається у складних умовах політичної нестабільності, воєнної агресії з боку РФ та

необхідності модернізації державного управління відповідно до стандартів Європейського Союзу. Розвиток електронного урядування в Україні проходив послідовні етапи, які охоплювали створення базових веб-присутностей органів влади, впровадження інтерактивних сервісів, запуск транзакційних платформ (портал «Дія»), а також спроби переходу до трансформаційного рівня, що передбачає персоналізовані послуги та повну цифрову інтеграцію процесів. Перелік базових державних послуг, які повинні бути доступні в цифровому форматі був визначений на основі однієї з ключових ініціатив Європейського Союзу у цій сфері, а саме Плану дій eEurope 2005, представлений Європейською Комісією у 2002 році [80]. Цей документ задекларував перелік з 20 основних публічних послуг, які рекомендовано надавати в електронному вигляді, зокрема 12 для громадян і 8 для бізнес-структур [80].

До переліку послуг для громадян увійшли такі сфери, як податкова звітність (декларація податку на доходи фізичних осіб), державна служба зайнятості (пошук роботи), доступ до соціальних виплат, оформлення особистих документів (паспорти, водійські посвідчення), реєстрація транспортних засобів, подання заяв на будівництво, повідомлення до поліції, послуги публічних бібліотек, отримання свідоцтв про народження та шлюб, подання заяв на вступ до вищих навчальних закладів, повідомлення про зміну адреси та доступ до базових медичних послуг.

Для бізнесу були визначені такі пріоритетні напрями електронного обслуговування як, сплата соціальних внесків за працівників, корпоративне оподаткування, подання звітності з ПДВ, реєстрація підприємств, передача статистичної інформації, оформлення митних декларацій, отримання екологічних дозволів та участь у публічних закупівлі через електронні платформи.

Ця типологія послуг стала основою для розробки та реалізації стратегій цифровізації державного сектору в країнах-членах ЄС і в Україні, сприяючи стандартизації та інтероперабельності державних сервісів, а також

розширенню доступу громадян і бізнесу до адміністративних процедур у зручному електронному форматі.

В свою чергу, Концепція розвитку електронного урядування в Україні, [39], визначає стратегічне бачення формування цілісної, ефективної та безпечної системи електронного урядування (рис.2.1).

У Концепції окреслено ключові вектори цифрової трансформації публічного управління, які мають на меті формування інтегрованої, прозорої та клієнтоорієнтованої моделі взаємодії держави з громадянами й бізнесом. Зокрема, передбачається формування єдиного цифрового простору шляхом забезпечення сумісності інформаційних систем, міжвідомчої взаємодії та використання централізованих електронних реєстрів, що дозволяє гармонізувати інформаційні потоки в межах органів влади.

Одним із важливих стратегічних напрямів визначено подальший розвиток електронних публічних послуг на основі підходу, орієнтованого на життєві ситуації користувача, що забезпечує не лише зручність та інклюзивність, а й підвищення рівня задоволеності громадян. Важливе місце відведено впровадженню електронної ідентифікації та засобів електронного підпису, що є основою цифрової довіри в системі публічних транзакцій.

У межах Концепції наголошено також на необхідності розбудови інфраструктури відкритих даних, зокрема шляхом створення умов для публікації урядової інформації у стандартизованих машиночитаних форматах, що відповідає вимогам прозорості та підзвітності органів влади.

Рисунок 2.1. Напрями розвитку електронного урядування України згідно з Концепцією

Джерело: систематизовано і побудовано автором на основі [42]

Окремим пріоритетом визначено посилення інформаційної безпеки у сфері електронного урядування. Зокрема, йдеться про створення нормативних засад для захисту персональних даних, а також розробку національних стандартів інформаційної безпеки, які б відповідали міжнародним зобов'язанням України. У Концепції також враховано потребу у цифровій конвергенції з Європейським Союзом шляхом уніфікації стандартів, що регламентують функціонування електронного уряду та обмін даними між державами.

Очікувані результати реалізації Концепції охоплюють як інституційні, так і практичні зміни. Серед них забезпечення повного доступу громадян і суб'єктів господарювання до основних адміністративних послуг в електронній формі, впровадження ефективних механізмів міжвідомчої взаємодії, зменшення бюрократичного навантаження, економія ресурсів та підвищення рівня довіри до держави. Окремо наголошено на меті підвищення позицій України в міжнародних рейтингах електронного урядування, що засвідчить зростання інституційної спроможності та цифрової зрілості публічного сектору [39].

Попри наявність чітких орієнтирів, практичне впровадження положень Концепції стикається з низкою викликів. У червні 2018 року Світовим банком було проведено комплексне оцінювання стану розвитку електронного урядування в Україні у форматі звіту Ukraine e-Government Assessment [118]. Аналіз базувався на методології Electronic Government's Governance Outline (eGGO), розробленій для вимірювання стану та динаміки цифрової трансформації в публічному секторі. Метою дослідження було виявити прогалини, бар'єри та потенційні напрями посилення і прискорення реформи електронного урядування, яка розглядається як ключовий елемент модернізації державного управління.

Звіт здійснював аналіз 18 індикаторів, згрупованих у 5 сфер, включно з політикою і плануванням, публічними послугами, даними та аналітикою, інфраструктурою й безпекою, а також механізмами контролю (Додаток В). За

результатами оцінювання, Україна перебувала на рівні «follower» - тобто держава з базовими напрацюваннями у сфері цифровізації, проте із суттєвими структурними обмеженнями [118].

У контексті нашого дослідження, саме категорії інфраструктури та безпеки, а також контрольних механізмів мають особливе значення (Додаток В). Найбільш значущі розриви між фактичним станом та прогнозними показниками спостерігаються у сфері забезпечення інформаційної безпеки, неперервності діяльності, моніторингу і контролю та перехресних перевірок. Це засвідчило недостатній рівень розвитку систем інформаційної безпеки в порівнянні із запланованими цілями. Така ситуація вказала на необхідність посилення зусиль щодо розвитку ефективних механізмів захисту інформації та удосконалення стратегій реагування на кіберзагрози.

Водночас у таких сферах, як платформи та послуги, ідентифікація користувачів, доступність послуг та взаємодія з користувачами, спостерігається суттєво менший розрив між реальними та запланованими результатами, що свідчить про відносно успішну імплементацію цифрових сервісів в Україні. Загалом цей аналіз підкреслює, що в процесі подальшого розвитку системи електронного урядування необхідно особливу увагу приділити питанням інформаційної безпеки, забезпечення надійної цифрової інфраструктури та створення дієвих контрольних механізмів, що дозволить підвищити не лише ефективність цифрових сервісів, а й довіру громадян до системи електронного урядування загалом.

Серед досягнень було відзначено запровадження системи Trembita (інтероперабельна платформа на зразок естонської X-Road), розвиток відкритих даних, функціонування порталів надання електронних послуг, а також прогрес у сфері кібербезпеки та нормативного регулювання. Однак низка критичних функціональних зон залишалася вразливою, серед них відсутність консолідованих дата-центрів, слабкий розвиток аналітики на основі даних, неефективна ІКТ-політика щодо державних закупівель,

відсутність єдиного підходу до управління життєвим циклом інформаційних систем, фрагментація реєстрів тощо [118].

Звіт 2018 року мав велике значення як передумова для системного вдосконалення елелктронного урядування в Україні. Його результати стали аналітичною основою для подальшого формування політик інтеграції в європейський цифровий простір, а також реалізації проектів на кшталт TAPAS та EGOV4UKRAINE. Ключовими рекомендаціями були розмежування функцій політики і реалізації, консолідація дата-центрів, підвищення ролі аналітики на основі даних, а також розробка спеціалізованої ІКТ-політики закупівель на державному рівні. Цей аналіз заклав стратегічне підґрунтя для переходу від фрагментарних ініціатив до цілісної архітектури цифрового уряду, орієнтованого на прозорість, ефективність та інноваційність. Його висновки залишаються релевантними у контексті оцінки динаміки реформ у 2020 - 2024 роках і визначення подальших кроків на шляху цифрової трансформації державного управління в Україні.

Аналіз даних Всеукраїнського опитування, проведеного Київським міжнародним інститутом соціології у 2023 році на замовлення ПРООН [61], свідчить, що рівень користування державними електронними послугами в Україні демонструє позитивну динаміку. Зокрема, 64% українців користувалися електронними послугами протягом 2023 року, тоді як у 2020 році ця частка становила лише 32%. Зокрема, близько 84% респондентів, які мали досвід користування такими сервісами, оцінили його як позитивний або переважно позитивний, що свідчить про зростання довіри до цифрових інструментів взаємодії з державою. Для порівняння, аналогічний показник у 2023 році становив 78,5%, що підтверджує сталу тенденцію до покращення сприйняття цифрових послуг серед громадян [61].

Більш ніж половина опитаних ідентифікували електронні сервіси як найбільш зручний та ефективний спосіб отримання адміністративних послуг. Водночас 31% респондентів зазначили, що їм комфортно користуватися як онлайн-платформами, так і фізичними сервісними центрами, зокрема

центрами надання адміністративних послуг (ЦНАП). Важливо зазначити, що 11% учасників опитування продовжують віддавати перевагу традиційній формі звернення до ЦНАП замість використання цифрових інструментів [61].

У 2024 році середньостатистичний громадянин України скористався 2,5 державними електронними послугами (рис.2.2).

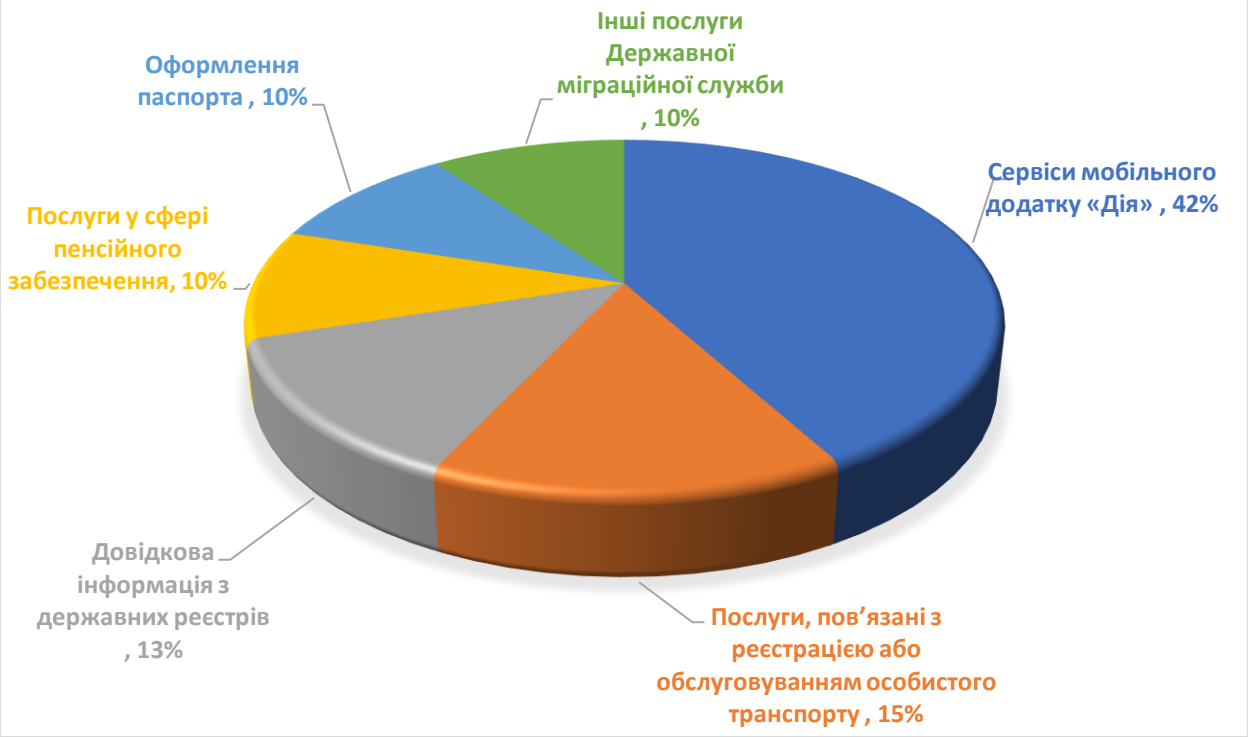


Рисунок 2.2. Структура електронних послуг наданих громадянам України у 2024 році

Джерело: побудовано автором на основі [61]

Найбільшою популярністю користуються сервіси мобільного додатку «Дія» (42% опитаних). Серед інших затребуваних послуг варто відзначити послуги, пов'язані з реєстрацією або обслуговуванням особистого транспорту (15%), отримання довідкової інформації з державних реєстрів (13%), послуги у сфері пенсійного забезпечення (10%), оформлення паспорта (10%) та інші дії в системі Державної міграційної служби (10%) [61]. Такі показники свідчать про поступову інституційну зрілість цифрових сервісів держави, а також про підвищення рівня цифрової компетентності громадян. Вони також

підкреслюють необхідність подальшого розширення доступності та функціональності електронних послуг, особливо для вразливих верств населення та мешканців віддалених регіонів.

Проте серед бар'єрів лишається низький рівень цифрових навичок, обмежений доступ до пристроїв та недовіра до цифрових сервісів. Лише 44% осіб віком 70+ років користуються інтернетом щодня, порівняно з 98% серед молоді до 30 років [61]. 27% опитаних назвали відсутність навичок основною причиною уникнення користування електронними послугами [61]. Згідно з дослідженням «Цифрова грамотність населення України 2023», проведеним Міністерством цифрової трансформації України, відзначено позитивну динаміку у формуванні цифрових навичок серед громадян. Зокрема, 93% дорослого населення віком 18-70 років володіють цифровими навичками, що на 8% більше порівняно з 2019 роком. Серед підлітків віком 10-17 років цей показник становить 95%, а серед осіб з порушенням слуху - 99% [94].

Найбільш розвиненими є інформаційні та комунікаційні навички - 79,2% та 78,9% відповідно мають рівень вище базового. Однак, навички вирішення життєвих проблем мають лише 55,8% та створення цифрового контенту - 36,8% залишаються на нижчому рівні [94].

Важливим аспектом є зростання обізнаності щодо безпеки в Інтернеті. З 2019 року на 11% збільшилася кількість осіб, які стикалися з проблемами, пов'язаними з безпекою в Інтернеті. Зокрема, 45,7% опитаних повідомили про випадки шахрайства в мережі [94]. Пандемія COVID-19 сприяла активнішому використанню цифрових технологій. Близько 52% українців вперше скористалися онлайн-інструментами, такими як онлайн-покупки, дистанційна робота та відстеження новин в Інтернеті [94]. Щодо навчання, 44,4% дорослого населення виявили зацікавленість у підвищенні цифрових навичок. Серед підлітків цей показник становить 71%, а серед осіб з порушенням слуху - 52,4% [94].

Партнерська Рамкова програма співпраці України з ООН на 2023-2027 роки акцентує увагу на важливості цифрової трансформації публічного

сектору, зокрема у контексті досягнення Цілей сталого розвитку. Згідно з документом, одним з ключових очікуваних результатів є формування ефективних, підзвітних та інклюзивних інституцій, здатних забезпечити належне урядування, дотримання прав людини і гендерної рівності. Впровадження цифрових платформ в управлінні має стати інструментом зміцнення довіри громадян до держави, забезпечення доступу до правосуддя та справедливих послуг [55].

Для забезпечення об'єктивної оцінки динаміки розвитку електронного урядування в Україні нами було проведено порівняльний аналіз глобального індексу розвитку електронного урядування (EGDI) та його складових на основі звітів ООН за чотири останні звітні періоди (2018, 2020, 2022 та 2024 роки) [111, 112, 113, 114]. Значення EGDI, як інтегрального показника, відображає рівень зрілості національної цифрової політики в контексті надання електронних публічних послуг, розвитку відповідної інфраструктури та цифрових компетентностей населення. Індекси, що його формують, дозволяють детальніше охарактеризувати сильні й слабкі сторони національних моделей е-врядування. Такий аналіз дозволив виявити ключові тенденції трансформації цифрового врядування, порівняти позиції України з державами-лідерами, а також з Грузією, країною яка має відносно схожий тренд розвитку електронного урядування з Україною.

У таблиці, наведеній нижче, представлено відповідні дані по Україні, Грузії, а також по провідних країнах цифрового врядування (Данія, Сінгапур, Південна Корея, Естонія, Великобританія, Швеція, Німеччина, Франція, США) і консалідований показник по країнах Європейського Союзу. Це дозволяє не лише оцінити позицію України у глобальному вимірі, а й виокремити напрями, які потребують подальшого розвитку (табл.2.1).

Таблиця 2.1. Динаміка Індексу розвитку електронного урядування за окремими країнами

Країна	2018	2020	2022	2024	Складові EGDI 2024		
					OSI (індекс онлайн послуг)	TII (індекс телекомунікаційної інфраструктури)	HCI (індекс людського капіталу)
Україна	**0,616**	**0,711**	**0,802**	**0,884**	**0,965**	**0,842**	**0,824**
ЄС (консолідований)	0,7727	0,817	0,8305	0,889	0,93	0,861	0,876
Данія	0,915	0,975	0,971	0,9847	0,99	0,996	0,958
Сінгапур	0,881	0,915	0,913	0,968	0,983	0,988	0,936
Південна Корея	0,901	0,956	0,952	0,967	1	0,991	0,912
Великобританія	0,899	0,935	0,913	0,957	0,953	0,974	0,945
Швеція	0,888	0,936	0,941	0,932	0,883	0,986	0,927
Естонія	0,848	0,947	0,939	0,97	0,995	0,973	0,949
Німеччина	0,876	0,852	0,877	0,938	0,923	0,923	0,967
США	0,876	0,909	0,915	0,919	0,913	0,96	0,884
Франція	0,879	0,871	0,883	0,874	0,844	0,922	0,856
Грузія	0,689	0,717	0,75	0,779	0,565	0,907	0,865

Джерело: систематизовано і складено автором на основі [111, 112, 113, 114]

Упродовж останніх років Україна демонструє стійке зростання за глобальним індексом розвитку електронного урядування, що підтверджується даними звітів ООН за 2018, 2020, 2022 та 2024 роки. У 2018 році значення EGDI для України становило 0,616, що відповідало нижчому середньосвітовому рівню. Проте вже у 2020 році показник зріс до 0,711, а у 2022 році - до 0,802. У 2024 році індекс сягнув позначки 0,884, що дозволило Україні увійти до групи країн з дуже високим рівнем розвитку електронного урядування та зайняти 30-те місце у глобальному рейтингу [114].

Аналіз динаміки індексу розвитку електронного урядування у 2018-2024 роках, представлений на рисунку 2.3, свідчить про стабільне зростання цифрової трансформації в Україні. У порівнянні з країнами-лідерами - Данією, Сінгапуром, а також із консолідованим показником по Європейському Союзу, - Україна демонструє не лише позитивну тенденцію, а й найбільш динамічну траєкторію зростання.

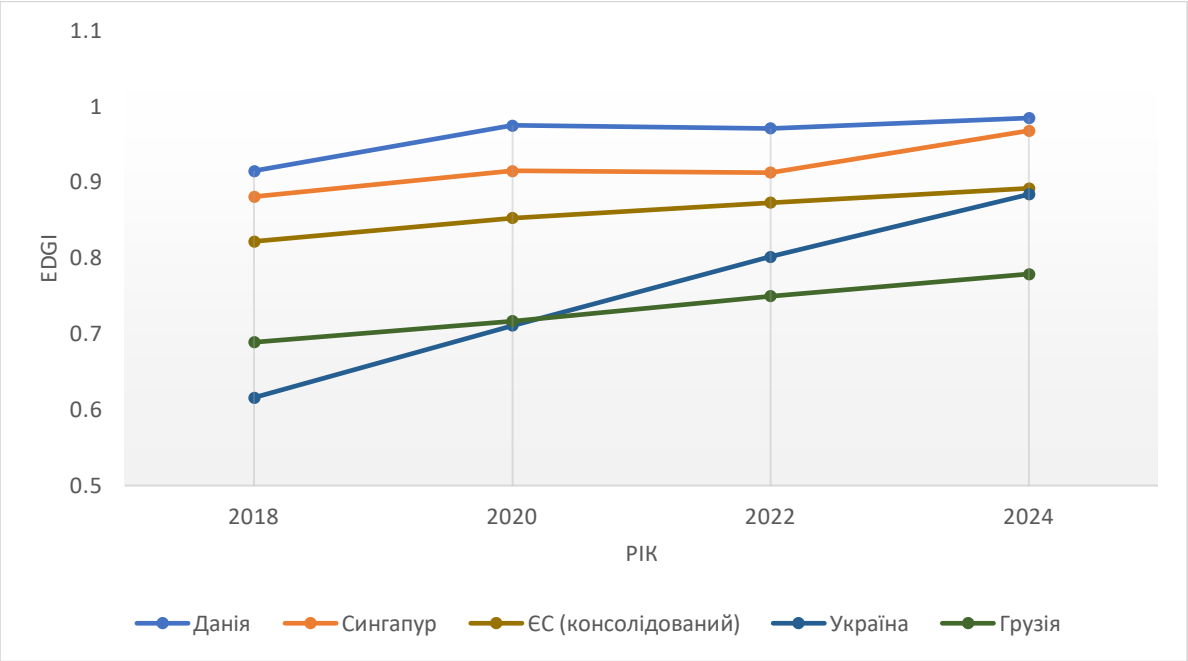


Рисунок 2.3. Динаміка індексу розвитку електронного урядування в порівнянні з іншими країнами у 2018-2024 роках

Джерело: побудовано автором на основі [111, 112, 113, 114]

Як видно з графіку, Данія, Сінгапур і ЄС мають високі початкові значення EGDI, що зумовлено вже наявною розвиненою цифровою інфраструктурою, комплексними державними політиками та стійкими традиціями електронного врядування. Їхні темпи приросту EGDI протягом аналізованого періоду є відносно стабільними, але помірними - коливаються в межах 0,05-0,07 пунктів.

На цьому тлі особливо вирізняється динаміка України, зростання відбулось на 0,268, що є найвищим приростом серед усіх представлених країн. Більш стриману динаміку демонструє Грузія, яка має близькі до України стартові позиції, однак відстає за темпами зростання.

Порівняння динаміки EGDI України з іншими державами дозволяє зробити висновок про істотне зближення із середньоєвропейськими стандартами. Так, у 2024 році середнє значення індексу EGDI по Європейському Союзу становило 0,892, що несуттєво перевищує український

показник. Для порівняння, Франція мала EGDI на рівні 0,874, Швеція - 0,932, а Німеччина - 0,938. Таким чином, Україна впритул наблизилася до провідних цифрових демократій і демонструє потенціал для подальшого входження до топ-20 світового рейтингу.

Окремо проаналізуємо складові EGDI, а саме індекс онлайн-послуг (OSI), телекомунікаційної інфраструктури (TII) та людського капіталу (HCI) за період 2008-2024 рр. (рис.2.4).

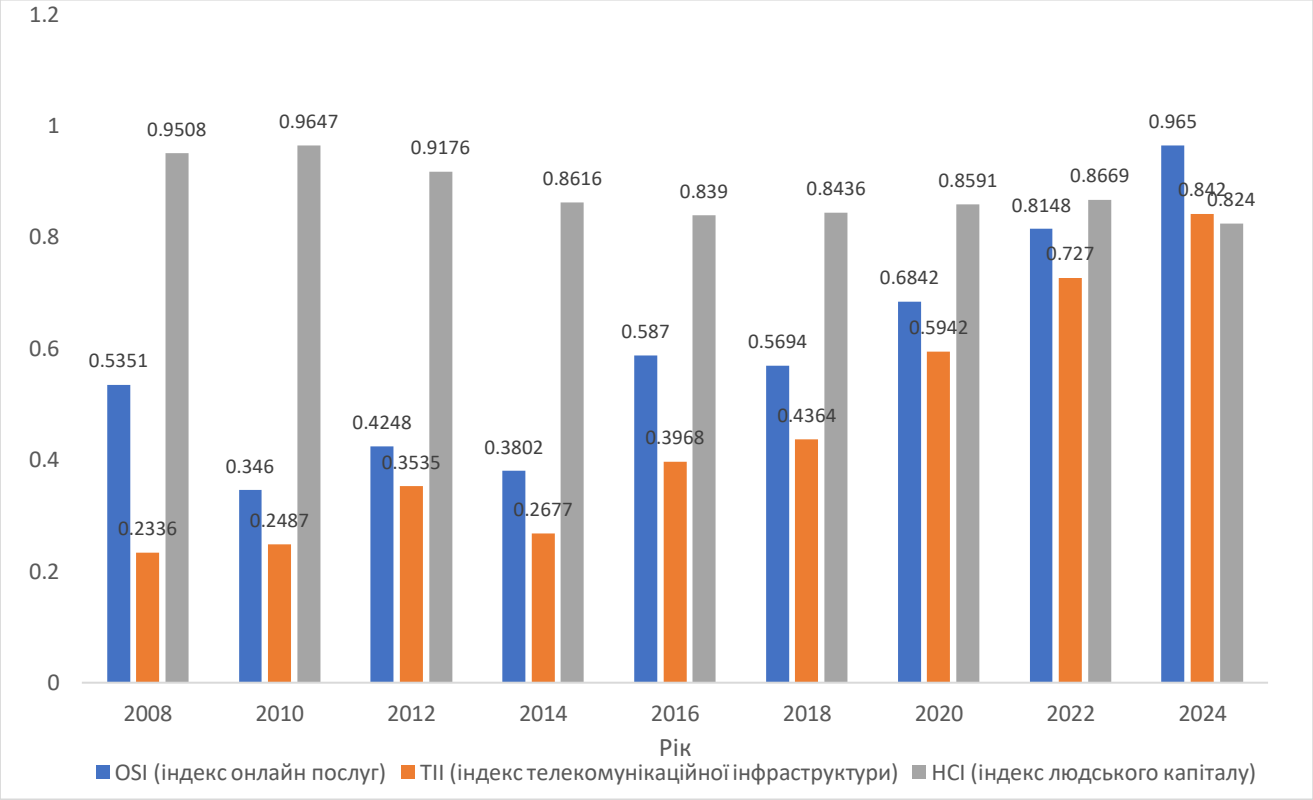


Рисунок 2.4. Динаміка складових Індексу розвитку електронного урядування за період 2008-2024 рр.

Джерело: систематизовано і побудовано автором на основі [110]

Аналіз складових EGDI свідчить про суттєвий прогрес у розвитку онлайн-послуг. Найбільш виражена позитивна тенденція проявляється в зростанні індексу онлайн-послуг. З 2008 року, коли цей індекс становив лише 0,5351, відбулось помітне і стабільне підвищення до 0,965 у 2024 році, що є одним із найвищих показників серед усіх країн-учасниць дослідження і

наближається до результатів лідерів рейтингу, таких як Естонія (0,995) чи Південна Корея (1,000). Таке суттєве зростання свідчить про інтенсивні кроки, які були здійснені українським урядом у сфері цифровізації адміністративних процедур і процесів. Це включає запровадження електронних послуг для громадян і бізнесу, інтеграцію інформаційних ресурсів, створення нових цифрових платформ, зокрема додатку «Дія», та перехід на електронну форму взаємодії між державою і громадянами. Водночас, активне зростання OSI свідчить не лише про кількісне збільшення онлайн-сервісів, але й про їх якісне удосконалення, що підтверджує підвищення загального рівня цифрових навичок та довіри населення до електронних послуг.

Індекс телекомунікаційної інфраструктури також демонструє послідовну позитивну динаміку протягом аналізованого періоду. У 2008 році цей показник мав найнижче значення - лише 0,2336, але до 2024 року зріс до 0,842, що хоча й залишається дещо нижчим за середній рівень країн Європейського Союзу (0,86). Але, такий приріст відображає значні інвестиції та зусилля у сфері розширення покриття інтернетом, розвитку мережевих технологій, впровадження сучасних стандартів зв'язку та мобільного інтернету. Ця динаміка є важливим фундаментом для розвитку електронного урядування, адже саме якісна телекомунікаційна інфраструктура забезпечує технічну основу для ефективного впровадження цифрових технологій у державному управлінні.

Однак ситуація з індексом людського капіталу характеризується неоднозначною динамікою. У 2008 році Україна мала досить високий початковий показник - 0,9508, досягнувши максимального значення 0,9647 у 2012 році. Проте, згодом спостерігається поступове коливання цього показника, з незначним падінням і повторним підвищенням, до 0,8824 у 2024 році. В цьому компоненті Україна ще поступається країнам із розвиненими моделями електронного урядування, зокрема Німеччині (0,967), Великій Британії (0,945) та США (0,884). Це вказує на існуючі проблеми та виклики у сфері освіти і професійної підготовки населення до цифрових трансформацій,

що підкреслює важливість запровадження системних освітніх реформ. Необхідною умовою подальшого прогресу є розвиток цифрової грамотності, компетенцій і навичок, що забезпечить сталий розвиток електронного урядування.

Ще одним важливим індексом в оцінці розвитку електронного урядування є Індекс електронної участі (E-Participation Index, EPI) він доповнює EGDI та дозволяє оцінити, наскільки громадяни залучені до процесів державного управління через цифрові технології. EPI характеризує рівень прозорості державних інституцій, ефективність комунікації з громадянами, активність останніх у процесах прийняття рішень та формуванні політики, а також ступінь їхньої цифрової взаємодії з владою (табл. 2.2).

Таблиця 2.2. Динаміка Індексу електронної участі за окремими країнами

Країна	2018	2020	2022	2024
Україна	**0,6854**	**0,8095**	**0,6023**	**1**
ЄС (консолідований)	0,8103	0,8095	0,6631	0,8025
Данія	1	0,9643	0,8864	0,9863
Сінгапур	0,9663	0,9762	0,9773	0,9589
Південна Корея	1	1	0,9432	0,9726
Великобританія	0,9831	0,9762	0,9545	0,9726
Швеція	0,9382	0,8214	0,7273	0,7945
Естонія	0,9101	1	0,9773	0,9589
Німеччина	0,9213	0,75	0,7273	0,9726
США	0,9831	1	0,9091	0,9452
Франція	0,9663	0,9048	0,7159	0,8082
Грузія	0,6236	0,6429	0,5341	0,5616

Джерело: систематизовано і складено автором на основі [111, 112, 113, 114]

Аналізуючи динаміку EPI України за період 2018-2024 років, можна відзначити суттєві коливання показників, які свідчать про неоднозначний характер процесу цифровізації публічного сектору та залучення населення до

електронної взаємодії з державою. У 2018 році показник EPI для України становив 0,6854, що відображало початковий етап розвитку цифрових інструментів взаємодії та низький рівень інтеграції громадськості у процеси електронного урядування.

У 2020 році спостерігається помітне зростання EPI до 0,8095, що було результатом активного впровадження таких ключових цифрових платформ, як застосунок «Дія», та інших сервісів для надання електронних послуг населенню. Також на це позитивно вплинула державна політика, спрямована на розширення прозорості та інтерактивності взаємодії державних органів із громадянами через електронні консультації та голосування, створення механізмів електронних петицій та відкритих даних.

Однак, вже у 2022 році спостерігалося суттєве зниження індексу до 0,6023. Причиною такого різкого падіння став початок повномасштабної війни, яка негативно вплинула на стан цифрової інфраструктури, призвела до суттєвих збоїв у роботі багатьох електронних сервісів, а також значно змінила пріоритети уряду щодо управління цифровими ресурсами. У цей період багато електронних послуг було призупинено або обмежено у функціонуванні, а увага уряду змістилася на забезпечення базової безпеки інформаційних систем, що знизило можливості громадян до активної участі через електронні платформи.

У 2024 році Україна демонструє стрімке покращення ситуації, досягаючи максимального показника EPI на рівні 1,0, який відповідає найвищим світовим стандартам і дозволяє країні увійти до лідерів рейтингу поряд з такими країнами, як Данія та Південна Корея. Таке значне підвищення показника пов’язано з кількома факторами. По-перше, після викликів 2022 року урядом було здійснено масштабну модернізацію цифрової інфраструктури з урахуванням міжнародних стандартів інформаційної безпеки. По-друге, активно розширено функціонал та інтерактивність існуючих цифрових платформ, особливо додатку «Дія», що дозволило значно посилити залученість громадян у державні процеси через інструменти

електронних консультацій, голосувань, опитувань та участі у формуванні державної політики. Крім того, громадяни почали частіше користуватися цифровими каналами зв'язку з державними органами, що підвищило загальний рівень цифрової довіри до уряду.

Порівняно з Грузією, яка протягом зазначеного періоду не змогла досягти суттєвих змін у своїх показниках (0,5616 у 2024 році), Україна демонструє виразну позитивну динаміку. Це свідчить про успішність стратегії уряду України щодо інтеграції сучасних цифрових технологій у сферу державного управління, ефективність заходів з подолання наслідків війни та відновлення повноцінної роботи цифрових сервісів. Трансформація України із держави з фрагментарним електронним урядуванням у державу з високим рівнем цифрової взаємодії між владою, громадянами та бізнесом, є вагомим свідченням інституційної спроможності держави до системної цифровізації управлінських процесів. Це створює сприятливі передумови для подальшого розвитку цифрового урядування відповідно до найкращих світових практик.

Все вище наведене засвідчує наявність суттєвого прогресу в цифровій трансформації вітчизняного публічного сектору. Протягом останніх років Україна пройшла шлях від фрагментарного застосування цифрових сервісів до формування комплексної системи електронної взаємодії держави, громадян і бізнесу.

Водночас, зберігаються окремі проблеми, які стримують подальшу інтеграцію електронного урядування. До таких належать недостатня цифрова інфраструктура в окремих регіонах, нерівномірність цифрових навичок серед населення, особливо серед літніх осіб, та фрагментованість інформаційних систем, що ускладнює реалізацію повної інтероперабельності, брак стратегічного планування, обмеженість аналітики на основі даних, а також потребу у спеціалізованій ІКТ-політиці закупівель на рівні держави [118].

Враховуючи зростання цифрової компетентності громадян і зростаючий попит на онлайн-сервіси [61], а також стратегічну орієнтацію України на європейську інтеграцію, подальший розвиток електронного урядування має

здійснюватися на засадах інклюзивності, відкритості, кіберстійкості та персоналізації послуг. Серед перспективних напрямів варто виокремити розбудову цілісної цифрової архітектури управління з єдиними реєстрами, дата-центрами та інтегрованими сервісами; запровадження національних стандартів кіберзахисту відповідно до міжнародних підходів; посилення захисту персональних даних та впровадження принципів цифрової довіри; активізацію цифрової освіти та формування культури цифрової безпеки; розширення механізмів електронної участі та підзвітності органів влади. Ефективна реалізація потенціалу електронного врядування потребує системного поєднання політичної волі, технологічної модернізації, нормативної адаптації та орієнтації на користувача, що дозволить Україні інтегруватися до кола цифрових демократій світу і перейти на рівень цифрового уряду.

Зростання обсягів електронних сервісів і збільшення обсягу оброблюваних даних актуалізують питання інформаційної безпеки як базового чинника стійкості та довіри до електронного урядування. У цьому контексті важливим є системний аналіз ризиків і загроз інформаційній безпеці, з якими стикається електронне урядування України на сучасному етапі.

2.2. Аналіз загроз та ризиків інформаційної безпеки в електронному урядуванні

Стрімка цифровізація державних сервісів супроводжується зростанням кіберзагроз і ризиків для інформаційної безпеки. Забезпечення конфіденційності, цілісності та доступності даних в електронних системах набуло критичної важливості, особливо в умовах воєнного стану. Під час повномасштабної агресії проти України кіберпростір став фронтом дій зловмистників, що здійснюють атаки, спрямовані на дестабілізацію ситуації, компрометацію державних ресурсів та отримання несанкціонованого доступу до інформації. В цих умовах аналіз загроз і ризиків інформаційної безпеки в

електронному урядуванні є вкрай актуальним завданням, від вирішення якого залежить стійкість цифрової держави та довіра громадян.

Загрози інформаційній безпеці в електронному урядуванні доцільно аналізувати, виходячи з їхнього походження - поділяючи їх на внутрішні та зовнішні (рис.2.5).

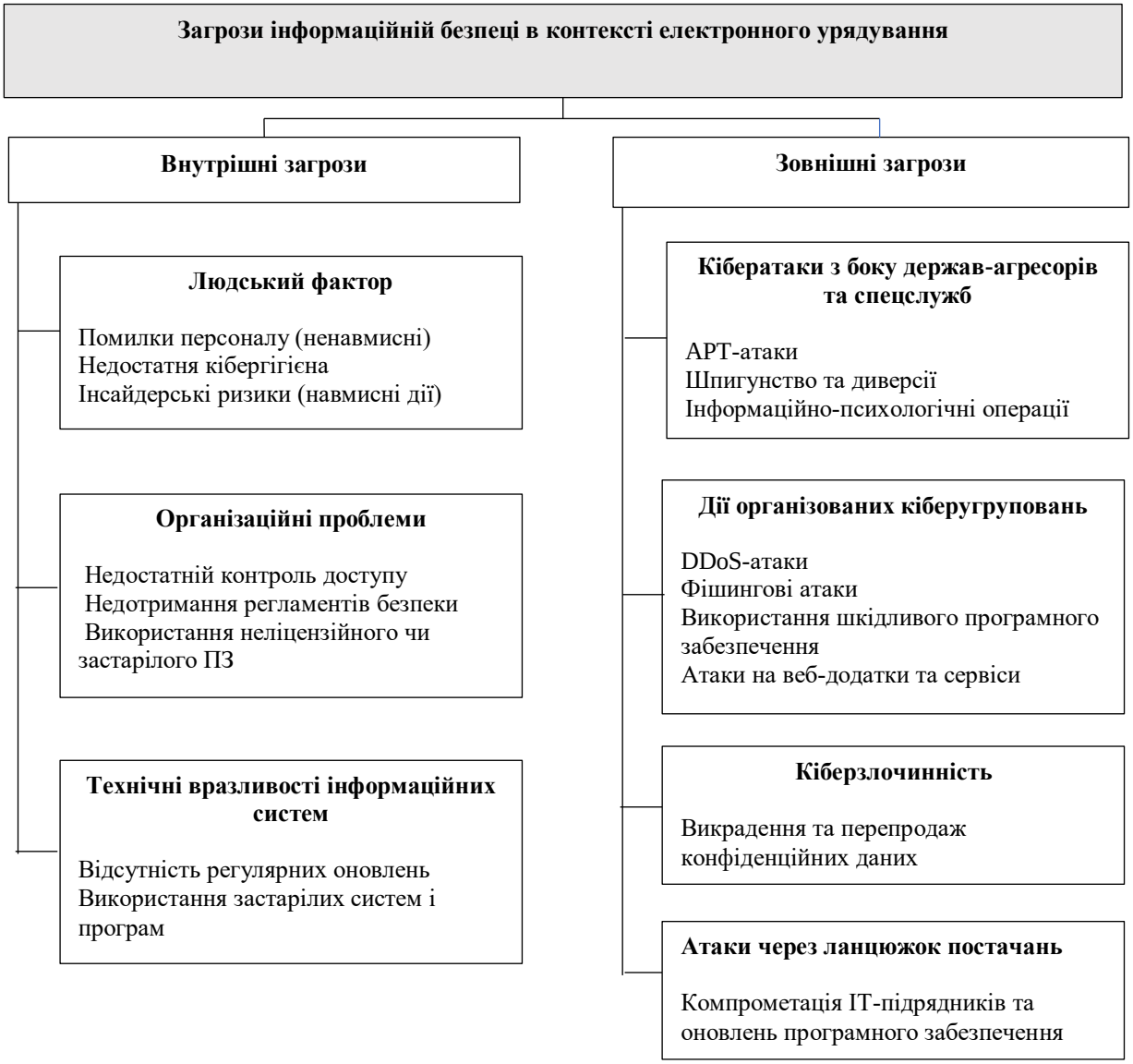


Рисунок 2.5. Структура загроз інформаційній безпеці електронного урядування

Джерело: побудовано автором на основі [7, 46, 118]

Така класифікація дозволяє більш точно визначити джерела та природу небезпек, зосередити увагу на слабких місцях системи захисту, що в свою чергу сприяє розробленню ефективних заходів із запобігання й протидії загрозам [7, 46, 118].

Внутрішні загрози, як правило, виникають всередині державних установ та можуть бути зумовлені людським фактором, організаційними недоліками або технічними вразливостями інформаційних систем [7, 46]. Врахування внутрішніх загроз дозволяє не лише виявити реальні недоліки у процесах організації роботи й захисту інформації, а й визначити необхідні заходи, зокрема навчання персоналу, формування культури кібербезпеки та внутрішнього контролю [118].

Зовнішні загрози мають принципово інший характер і пов’язані з діями таких сторонніх суб’єктів, як кіберзлочинців, організованих хакерських угруповань, спецслужб інших держав або навіть терористичних організацій. Такі загрози спрямовані на проникнення в державні інформаційні системи ззовні та включають широкий спектр атак: фішинг, шкідливе програмне забезпечення, DDoS-атаки, цілеспрямовані операції типу APT (Advanced Persistent Threat) [7, 118]. Аналіз зовнішніх загроз важливий, тому що він дозволяє визначити потенційні вектори атак, розробити методи протидії, а також оцінити ефективність наявних засобів кіберзахисту.

Поділ інформаційних загроз на внутрішні та зовнішні є науково та практично обґрунтованим, оскільки він враховує природу й джерела виникнення ризиків, що дозволяє комплексно підійти до забезпечення інформаційної безпеки в електронному урядуванні.

Одним із найсуттєвіших внутрішніх ризиків для інформаційної безпеки є людський фактор. Помилки персоналу, недостатня кібергігієна та зловживання доступом можуть призвести до інцидентів, навіть якщо технічні засоби захисту присутні. За оцінками експертів, до 98% усіх кібератак так чи інакше експлуатують уразливості, пов’язані з людським фактором, і розраховані на дії непідготовленого користувача [93]. Це означає, що

ненавмисна помилка співробітника (наприклад, перехід за фішинговим посиланням або використання слабкого пароля) може стати початковою точкою компрометації державної інформаційної системи.

До внутрішніх загроз також належать інсайдерські ризики - навмисні дії працівників чи підрядників, які мають доступ до ІТ-інфраструктури органів влади. Це може бути витік конфіденційних даних, саботаж або встановлення шкідливого програмного забезпечення зсередини. Людський фактор доповнюється організаційними проблемами: недостатня підготовка кадрів з кібербезпеки, відсутність належного контролю доступу та аудиту дій користувачів, а також недотримання юридичних регламентів інформаційної безпеки. Несвоєчасне встановлення оновлень безпеки чи використання неліцензійного програмного забезпечення можуть створювати вразливості ІТ-інфраструктури, які зловмисники легко експлуатують. Нерідко державні установи використовують застарілі системи або програмні продукти, що більше не підтримуються виробниками, такі компоненти стають «слабкою ланкою» захисту. Внутрішні недоліки організації інформаційної безпеки підсилюють наслідки зовнішніх атак, тому держава повинна приділяти увагу навчанню персоналу та внутрішньому контролю.

Зовнішні загрози є багатогранними - від технічних можливостей віддаленого несанкціонованого доступу до психологічних операцій - і потребують комплексної протидії. Зовнішні кіберзагрози щодо електронного урядування України походять від різних суб’єктів - від держав-агресорів і їхніх хакерських угруповань до кіберзлочинців та шахраїв [57]. Найбільш потужні та скоординовані атаки пов’язані з діяльністю російських спецслужб, які розглядають українське електронне урядування як ціль для шпигунства, диверсій та інформаційних операцій. За даними Служби безпеки України, кількість російських кібератак стрімко зросла за останні роки, з 1400 у 2021 році до приблизно 4500 у 2022-му, і на такому ж рівні залишалася у 2023 році [63]. Загалом з початку повномасштабної війни (2022-2023) СБУ зафіксувала понад 9000 кібератак російського походження [63]. Така масштабна і

безпрецедентна кіберагресія створює постійну зовнішню загрозу для державних електронних ресурсів.

Зловмисники використовують широкий спектр векторів атак, підбираючи методи залежно від мети та вразливостей електронних ресурсів. Серед типових технік, з якими стикалася Україна, можна виділити [57]:

1. Фішингові атаки - масове або таргетоване розсилання підроблених повідомлень від імені легітимних організацій з метою викрадення облікових даних чи встановлення шкідливого ПЗ. Фішинг залишається одним із найпоширеніших методів отримання початкового доступу до внутрішніх систем державних органів [65]. Варто зазначити, що цільовий фішинг застосовується проти конкретних державних посадовців з доступом до критичних систем, аби обійти загальні захисні фільтри.

2. Шкідливе програмне забезпечення - після проникнення в мережу хакери завантажують віруси, трояни, бекдори. Урядові системи України неодноразово уражалися такими програмами, які знищують дані. Показовим інцидентом стала атака в ніч на 14 січня 2022 року, коли одночасно було зламано десятки державних сайтів, у тому числі портал «Дія», на їхніх головних сторінках розмістили провокаційне повідомлення, а в фоновому режимі вірус WhisperGate видалив дані на серверах [8]. Держспецзв'язок офіційно підтвердив, що дефейс вебсайтів і знищення інформації були частиною однієї масштабної кібератаки, спрямованої на завдання максимальної шкоди інфраструктурі державних електронних ресурсів [8]. Цей випадок продемонстрував новий рівень координації дій зловмисників - комбінування інформаційно-психологічного тиску, демонстративний злам сайту із прихованим нищенням критично важливих даних.

3. Атаки на веб-додатки та сервіси - вразливі вебпортали органів влади стають легкою мішенню. За статистикою CERT-UA, серед інцидентів 2021 року найбільш поширеними були спроби проникнення та втручання в роботу сайтів, сканування web-застосунків, а також ін'єкції та інші атаки на web-сервери [71].

Неправильно налаштовані сервери можуть призвести до витоку даних з державних реєстрів або до несанкціонованого доступу. У 2023 році кібератака на дата-центр «Парковий» дозволила зловмисникам проникнути в IT-інфраструктуру, що обслуговує десятки державних компаній, через що тимчасово не працювали сервіси «Нафтогазу», «Укрпошти», «Укрзалізниці» та система електронного перетину кордону «Шлях» [71]. Це свідчить про небезпеку ланцюгових реакцій через компрометацію одного вразливого вузла (хмарного чи дата-центру) на декілька електронних сервісів держави.

4. Атаки типу Distributed Denial of Service (DDoS) - масоване перевантаження трафіком вебпорталів або мережевих сервісів з метою виведення їх з ладу. У лютому 2022 Україна пережила найпотужнішу в своїй історії DDoS-атаку, спрямовану одночасно на сайти державних установ та банків [71]. Зловмисники намагалися паралізувати роботу порталів і посіяти паніку серед населення. За даними Міністерства цифрової трансформації, ця атака була завчасно підготовлена і мала на меті дестабілізацію фінансової та соціальної систем напередодні вторгнення [47]. Зусиллями фахівців з кібербезпеки в держорганах і банках удар вдалося відбити та відновити роботу сервісів упродовж кількох годин, але інцидент показав, що DDoS-атаки залишаються грізною зброєю у арсеналі агресора для тимчасового порушення надання електронних послуг.

5. Атаки через ланцюжок поставок - компрометація програмного забезпечення або IT-підрядників, що обслуговують державні органи. Такі атаки особливо небезпечні, оскільки можуть непомітно додавати несанкціонований віддалений доступ у широко використовувані продукти. В Україні фіксувалися спроби зламати компанії-розробники, аби через їхні оновлення отримати доступ до державних систем. Як приклад, у 2021 році було скомпрометовано мережу IT-компанії, що розробляла систему управління ресурсами для Міністерства оборони України [106]. Інше угруповання атакувало IT-фірми, які надавали аналогічні послуги державним замовникам і за кордоном. Ціль таких операцій - отримати плацдарм для

подальших ударів по державних установах через довірені програмні канали. Цей вектор вимагає особливої уваги, адже навіть повністю захищена урядова мережа може бути зламана, якщо використовується скомпрометоване програмне забезпечення.

Статистика останніх п’яти років демонструє різке зростання атак на державні інформаційні ресурси. За даними Держспецзв’язку, протягом 2022 року Україна зіткнулася з приблизно 7000 кібератак на свою інформаційну інфраструктуру, що в 2,8 раза більше, ніж у 2021 році [71]. Урядова команда реагування CERT-UA лише з кінця лютого до грудня 2022 опрацювала 2194 кіберінциденти [57] - неймовірна кількість, зумовлена початком повномасштабної війни. Відповідно, Україна стала однією з найбільш атакованих країн світу. У 2022-му загальна кількість кібератак зросла в 3,5 рази порівняно з попереднім роком, причому найчастіше під удари потрапляли саме державні установи та об’єкти критичної інфраструктури [106] (рис.2.6).

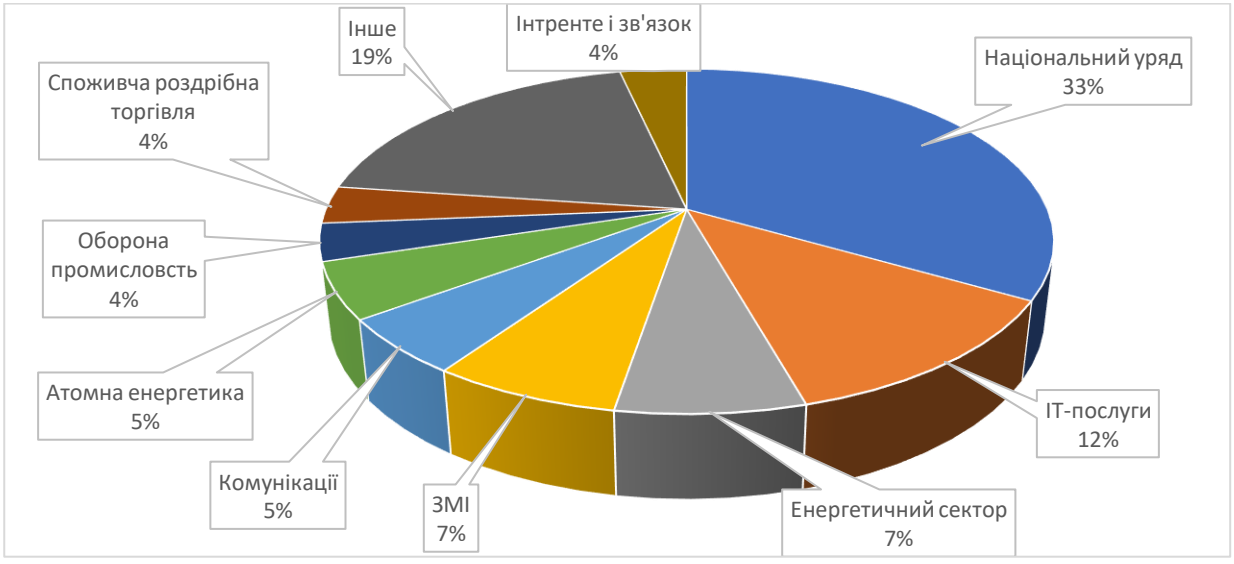


Рисунок 2.6. Розподіл кібератак у розрізі галузей промисловості під час російського вторгнення в Україну, 2022 рік

Джерело: побудовано автором на основі Special Report: Defending Ukraine - Early Lessons from the Cyber War [106]

Кіберпростір відображає перебіг воєнних дій, так в період лютий-квітень 2022 року російські хакери атакували майже всі ключові сектори критичної інфраструктури України, причому кібератаки майже завжди співпадали в часі з військовими операціями агресора [106]. Більше того, географія кібератак часто співвідносилася з регіонами активних бойових дій [106] (рис.2.7).

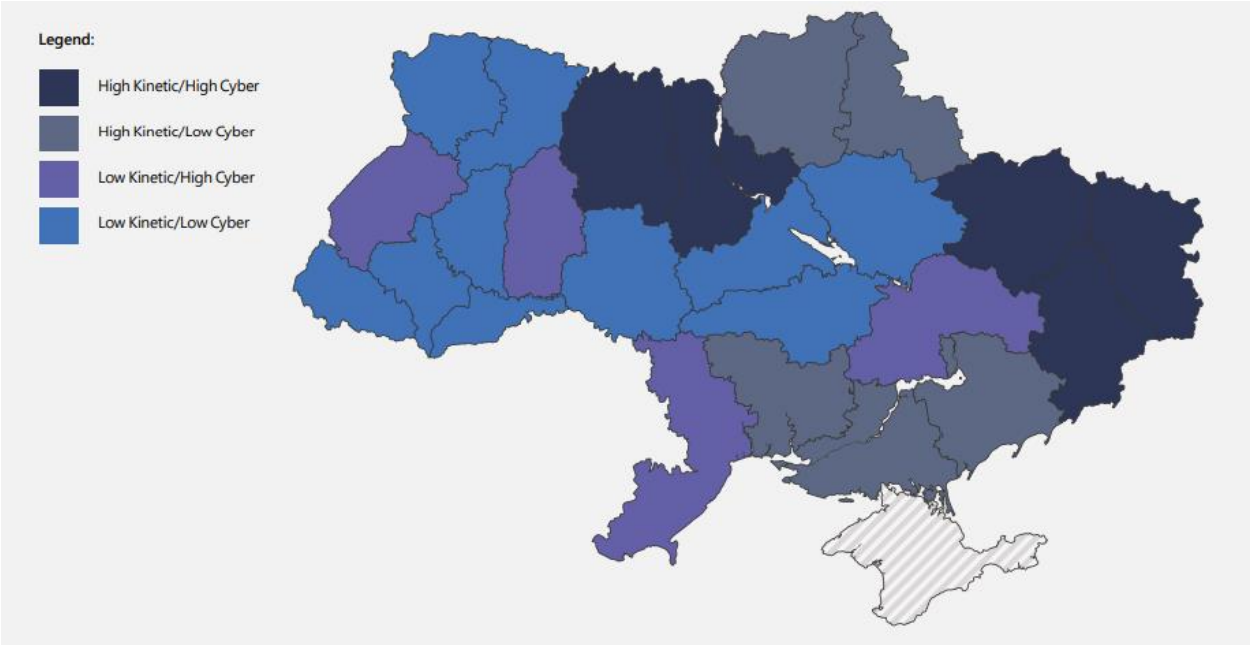


Рисунок 2.6. Розподіл кібер- і кінетичних військових дій в 2022 році
Джерело: [106, с.10]

Це підтверджує тезу про координацію кібероперацій із воєнними цілями. У перші тижні вторгнення фіксувалися масовані деструктивні атаки, так за період 23 лютого - 8 квітня 2022 щонайменше 40 результативних кібератак призвели до знищення файлів десятків українських організацій [106]. Для цього агресор застосував принаймні 8 різновидів руйнівних вірусів, що перезаписують дані і виводять з ладу комп'ютери [106]. Близько 40% цих деструктивних атак були спрямовані на об'єкти критичної інфраструктури, а 32% - на органи державної влади різного рівня [106]. Така хвиля безпрецедентних кібератак була покликана максимально дестабілізувати управління державою та ускладнити роботу електронних ресурсів у розпал

військового вторгнення. Попри екстремальне навантаження, державна система інформаційної безпеки України змогла витримати основний удар і продовжує нарощувати організаційно-технічні спроможності.

У 2023 році інтенсивність кібератак залишалася високою, хоча й дещо стабілізувалася порівняно з піком 2022-го. CERT-UA опрацювала 2543 кіберінциденти за 2023 рік - це на 15,9% більше, ніж у 2022 році [57]. Основними типами інцидентів у 2023 році були розповсюдження шкідливого програмного забезпечення, фішинг та інші види зловмисних підключень.

Варто наголосити, що в сучасних умовах кібератаки все більше перетворюються на інструмент інформаційно-психологічного впливу. Якщо раніше основною метою хакерів було тихе викрадення розвідувальних даних чи виведення з ладу окремих систем, то нині кібератаки часто мають на меті широкий суспільний резонанс. Сьогодні кібератаки стали складником спецоперацій країни-агресора і спрямовані на маніпуляцію суспільством, внутрішню дестабілізацію та дискредитацію органів влади. Прикладом є атака на найбільшого телекомунікаційного оператора «Київстар» у грудні 2023 року, яка не лише знищила значну частину IT-інфраструктури компанії, але й залишила без зв’язку понад 24 мільйони абонентів на кілька днів [63]. Попри те, що «Київстар» - приватна компанія, цей інцидент мав потужний негативний суспільний ефект, вплинувши на систему зв’язку країни вцілому. Все вище наведене підкреслює, що загрози інформаційній безпеці електронного урядування в умовах війни є критично високими. Україна стала своєрідним «полігоном» кібервійн, за час війни на її цифровий простір припало понад 600 суттєвих кібератак (близько п’ятої частини всіх у світі) [47].

Забезпечення інформаційної безпеки в електронному урядуванні залежить не лише від технологій, а й від наявності сучасної законодавчої бази та чітких процедур. В Україні сформовано базові засади кібербезпеки, а саме діє Закон «Про основні засади забезпечення кібербезпеки України» [25], затверджено Стратегію кібербезпеки, оновлену наприкінці 2021 року [60].

Були створені уповноважені органи Держспецзв'язку, Національний координаційний центр кібербезпеки при РНБО, підрозділи кіберполіції, кіберцентр СБУ тощо. Однак нормативно-правове поле все ще має суттєві прогалини, які знижують рівень захищеності цифрової держави [3]. Дослідження показують наявність низки проблем: законодавчі неузгодженості між різними актами, недостатнє регулювання окремих аспектів кібербезпеки та відсутність чітких механізмів захисту прав громадян у цифровому просторі [3]. Одним із прикладів законодавчих викликів є забезпечення інформаційної безпеки в органах місцевого самоврядування. Багато електронних послуг надаються на місцевому рівні через ЦНАПи чи муніципальні портали, але не всі громади мають ресурси і фахівців для виконання вимог кіберзахисту. Існуючі нормативні акти не завжди визначають відповідальність і порядок реагування на кіберінциденти для невеликих державних установ. Також потребує оновлення стандартна документація з технічного захисту інформації - багато відомчих інструкцій застаріли і не враховують сучасних загроз (хмарні технології, мобільні додатки, віддалена робота тощо).

Нормативне забезпечення електронного урядування має йти в ногу з технологічним розвитком. Проте в Україні цифрові сервіси часто впроваджуються швидше, ніж оновлюються закони. Це призводить до ситуацій, коли правове поле не покриває нові ризики. Наприклад, масове впровадження мобільного додатку «Дія» поставило питання захисту персональних даних у смартфонах громадян з боку провайдерів послуг. Закон «Про захист персональних даних» [18] поки не повністю узгоджений з європейськими стандартами (GDPR) і не враховує всіх нюансів дистанційної ідентифікації, що використовується в «Дії».

Ще один аспект - міжвідомчий обмін даними. Проекти на кшталт «Трембіта» (система обміну даними між держреєстрами) значно підвищили ефективність послуг, але одночасно створили залежність одних реєстрів від інших. У січні 2025 року НАЗК повідомило, що було змушене тимчасово призупинити роботу функції автозаповнення декларацій через масштабну

кібератаку на реєстри Міністерства юстиції, до яких НАЗК має автоматизований доступ [47]. Цей випадок вказує на необхідність координації безпеки між різними держателями інформації та передбачення правових процедур на випадок компрометації суміжних систем.

До проблем нормативного характеру слід віднести і питання інцидент-менеджменту та відповідальності. Хоча створено Національну телекоммережу та урядову команду реагування CERT-UA, не всі органи виконавчої влади чітко розуміють алгоритм дій при кібератаці. Формально відповідальність за кіберзахист розподілена між Держспецзв'язку, СБУ, НКЦК та іншими, але на практиці це може призводити до дублювання функцій чи прогалин. Потрібне вдосконалення підзаконних актів, які б регулювали обмін інформацією про кіберінциденти, обов'язкове повідомлення про критичні атаки, проведення аудиту безпеки в державних органах тощо. Експерти відзначають необхідність оновлення підходів до сертифікації засобів захисту, імплементації міжнародних стандартів (ISO/IEC 27001, NIST) у державному секторі та введення жорсткішої відповідальності за недотримання мінімальних вимог кібербезпеки [8, 47, 93].

Позитивним кроком стало затвердження Стратегії кібербезпеки України на 2021-2025 роки [66], яка визначає пріоритети і завдання у цій сфері. Зокрема, вона передбачає створення системи моніторингу кіберпростору, удосконалення нормативної бази, розвиток публічно-приватного партнерства і підготовку кадрів. У 2023 році уряд ухвалив план заходів на реалізацію Стратегії, що включає оновлення законодавства та впровадження нових стандартів захисту інформації. Проте реальне виконання цих заходів потребує ресурсів та політичної волі. Наявні виклики - воєнний стан, обмежене фінансування, пріоритетність воєнних потреб - впливають на темпи нормативних змін. Попри це, забезпечення кіберстійкості електронного урядування має залишатися одним з пріоритетів, адже від нього залежить безперервність управлінських процесів навіть у кризових ситуаціях.

Загрози інформаційній безпеці електронного урядування набули пікового значення під час воєнного стану. Кібератаки на державні ресурси прямо пов’язані із питаннями національної безпеки. Агресор намагається використати кіберпростір для досягнення військових та політичних цілей: посіяти хаос, порушити роботу урядових сервісів, позбавити громадян критичних послуг (зв’язку, банківських транзакцій, доступу до реєстрів) та підірвати довіру до влади. Особливо актуальним стало питання захисту державних реєстрів та баз даних. Більшість ключових реєстрів (громадян, юридичних осіб, нерухомості, фінансових транзакцій тощо) переведені в електронну форму, тому їх компрометація чи знищення може мати катастрофічні наслідки. Умовно кажучи, втрата чи фальсифікація даних реєстрів під час війни здатна паралізувати соціальні виплати, роботу держслужб, призвести до правового колапсу у питаннях власності. Це розуміють і противники - відомі спроби кібератак на Реєстр демографічного обліку, системи Казначейства, реєстри Мін’юсту. Друга критична ділянка - урядові вебресурси та системи зв’язку. Масові дефейси сайтів на початку 2022 року мали на меті підірвати довіру населення до електронного уряду та показати слабкість держави. Хоча витоку даних тоді не сталося, сам факт зламу урядових порталів викликав суспільний резонанс.

Зрозуміло, що воєнний час висвітив і загострив усі наявні проблеми інформаційної безпеки. Якщо раніше кібератаки могли сприйматися як суто технічний інцидент, то зараз вони безпосередньо впливають на обороноздатність, економіку та життя громадян. Кожен успішний напад на електронне урядування під час війни може бути використаний ворогом для підриву України. Водночас, український досвід кіберстійкості набуває світового значення - відбивати щодня складні атаки і зберігати функціонування цифрової держави в екстремальних умовах вдається дуже небагатьом країнам.

2.3. Аналіз нормативно-правового та інституційного забезпечення електронного урядування в контексті інформаційної безпеки

Електронне урядування в Україні регулюється комплексом законів і доктрин, що визначають обіг інформації, надання електронних послуг та забезпечення інформаційної безпеки. Водночас динамічний розвиток технологій і сучасні загрози ставлять питання відповідності чинного законодавства міжнародним стандартам та актуальним ризикам. Нормативно-правова база електронного урядування в Україні містить низку базових законодавчих актів. Вона почала формуватися з набуттям країною незалежності і продовжує трансформуватися у відповідь на виклики глобального середовища. Такі закони як, Закони України «Про інформацію» (1992) [20] та «Про доступ до публічної інформації» (2011) [15] заклали фундамент інформаційних правовідносин, визначивши право громадян на інформацію та обов'язки держави щодо прозорості. Закон України «Про інформацію» встановлює принципи відкритості, достовірності та повноти інформації, а Закон «Про доступ до публічної інформації» гарантує механізми отримання публічних даних на запити громадян, що відповідає демократичним стандартам прозорості влади.

В 2003 році було прийнято Закон України «Про електронні документи та електронний документообіг» [16], який запровадив правові засади використання електронних документів у діловодстві та наданні послуг. Він визначив юридичну силу електронного документа, за умови накладення електронного підпису, та регулював порядок обміну такими документами між установами і громадянами. Цей Закон фактично легітимував безпаперовий документообіг, створивши основу для розвитку електронних послуг. Важливо, що з метою наближення до європейських норм у 2022 році було прийнято нову редакцію законодавства про електронний документообіг, яка з 2023 року набрала чинності та гармонізувала українські правила з вимогами ЄС. Це

свідчить про постійне оновлення правового поля відповідно до сучасних тенденцій.

В сфері електронних послуг ключовим є також Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [17], який замінив собою попередній Закон «Про електронний цифровий підпис». Новий закон впровадив європейські стандарти (регламент eIDAS) у сфері електронної ідентифікації та підпису, забезпечивши взаємне визнання кваліфікованих електронних підписів і печаток. Він запровадив поняття таких кваліфікованих довірчих послуг, як електронний підпис, печатка, часова позначка тощо та створив правові умови для розвитку інфраструктури цифрової ідентифікації і автентифікації громадян. В результаті, Україна досягла значного прогресу і з 2023 року українські кваліфіковані електронні підписи внесені до довірчого списку ЄС [72], що означає їх визнання як удосконалених підписів у Євросоюзі. Це підтверджує відповідність вітчизняного законодавства європейським вимогам у цій сфері.

Для стратегічного розвитку цифрового суспільства було ухвалено Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Цей акт визначав пріоритети державної політики у запровадженні ІКТ в економіці, освіті, державному управлінні та інших сферах. Хоча дія цього закону формально обмежувалася 2015 роком, його принципи заклали основу для наступних стратегічних документів. Зокрема, уряд України у подальші роки затвердив Концепцію розвитку цифрової економіки та суспільства та Стратегію цифрової трансформації України, які стали продовженням реалізації політики цифровізації. Аналогічно, ще раніше, Закон України «Про Національну програму інформатизації» [23] і нова редакція Закону від 2023 року [84] визначив механізми планування та фінансування загальнодержавних проектів інформатизації. На підставі цього закону регулярно затверджуються Державні програми інформатизації (включаючи заходи з розвитку інтернет-інфраструктури, електронного урядування, створення реєстрів тощо). Проте реалізація цих програм

неодноразово стикалася з недофінансуванням та організаційними проблемами, що вказує на необхідність актуалізації підходів до інформатизації в умовах війни та обмежених ресурсів.

Невід'ємною складовою нормативного забезпечення є акти у сфері інформаційної безпеки, адже стале електронне урядування можливе лише за умови захищеності інформаційних ресурсів [50, 124]. Доктрина інформаційної безпеки України, стала реакцією держави на загрози гібридної агресії. Ця доктрина визнала критичними викликами поширення дезінформації, кібератаки на державні інформаційні системи та інші загрози інформаційному простору. В ній визначено такі стратегічні цілі, як захист національного інформаційного суверенітету, розвиток засобів кіберзахисту, протидія пропаганді та забезпечення кіберстійкості державних ресурсів. Доктрина 2017 року відповідала умовам того часу, проте повномасштабна війна 2022 року актуалізувала потребу в оновленні стратегічних підходів. Наразі пріоритетами залишаються ті самі напрями, але з більшим акцентом на кібероборону та міжнародну координацію.

Окрім спеціальної доктрини, питання інформаційної та кібернетичної безпеки відображені і в базових законах національної безпеки. У Законі України «Про основи національної безпеки України» (2003) [24] інформаційна безпека прямо визначалась одним із пріоритетів державної політики безпеки. З 2018 року діє Закон «Про національну безпеку України» [86], який інтегрував поняття кібербезпеки та захисту критичної інформаційної інфраструктури до загальної системи безпеки. Він заклав правові рамки для створення Національної системи кібербезпеки і координації між суб'єктами цієї системи.

В цілому, чинне законодавство у сфері електронного урядування є досить розгалуженим і охоплює як питання надання електронних послуг (е-документів, відкритих даних, електронної взаємодії), так і питання інформаційної безпеки. Багато норм були оновлені з огляду на європейську інтеграцію України. Зокрема, у сфері захисту персональних даних українське

законодавство поступово приводиться у відповідність із Загальним регламентом захисту даних ЄС (GDPR) [68].

Проте, як буде показано далі, існують і певні прогалини та застарілі положення, які потребують вирішення з урахуванням сучасних реалій. Попри наявність базових законів, ряд напрямів інформаційної безпеки в електронному урядуванні ще не до кінця врегульовано або стикається з прогалинами. Серед них можна виділити захист персональних даних, кіберзахист публічних електронних сервісів, використання хмарних технологій, правове поле для штучного інтелекту та питання цифрової ідентифікації громадян.

Чинний Закон України «Про захист персональних даних» [18] суттєво поступається сучасним європейським вимогам. Він був прийнятий на основі директив ЄС попереднього покоління і лише частково враховує стандарти GDPR. Наприклад, в ньому відсутні достатньо деталізовані норми про повідомлення про витоки даних, про право на перенесення даних, прозорість обробки та інші механізми, які в ЄС нині є обов'язковими. Крім того, інституційно в Україні довгий час не було незалежного органу захисту даних [124]. Функції нагляду виконував Уповноважений Верховної Ради з прав людини, що не повністю відповідало моделі самостійного Data Protection Authority [67]. Як наслідок, практика захисту персональних даних була слабкою, а саме фіксувалися численні випадки витоків інформації з державних реєстрів та баз, у тому числі через кібератаки, але притягнення до відповідальності було поодиноким.

Наразі ситуація змінюється, у жовтні 2022 року парламент прийняв у першому читанні нову редакцію закону про персональні дані (законопроєкт №8153) для повної імплементації норм GDPR. Цей законопроєкт покликаний усунути прогалини. Розширити права суб'єктів даних, встановити прозорі процедури обробки, створити окремий орган із захисту даних та запровадити значні штрафи за порушення. Сфера персональних даних перебуває у стадії реформування, і на час підготовки цього дослідження вона ще не повністю

відповідає європейському стандарту приватності, хоча кроки в цьому напрямі активно здійснюються.

Розвиток електронного урядування робить критично важливим питання стійкості та безпечності державних цифрових сервісів. Закон України «Про основні засади забезпечення кібербезпеки України» [29] визначив основні суб'єкти кібербезпеки та їх повноваження, але його реалізація виявила низку проблем. Зокрема, до 2022 року повільно здійснювалася класифікація об'єктів критичної інформаційної інфраструктури та аудит їх захищеності. Багато електронних ресурсів органів влади не мали актуальних комплексних систем захисту інформації або сертифікованих засобів кіберзахисту. Це призвело до того, що на початку 2022 року низка урядових сайтів постраждала від масованої кібератаки, яка стала прелюдією до військової агресії. Хоча критичні реєстри не були знищені, інцидент виявив вразливість в частині недостатньої координації дій та відсутності резервування даних за межами потенційної зони атаки [106]. В ході повномасштабної війни вдалося частково компенсувати ці недоліки. Завдяки екстреним заходам значна частина державних реєстрів була перенесена на захищені майданчики, здійснено резервне копіювання важливих баз даних, налагоджено цілодобовий моніторинг кіберінцидентів. Проте на нормативному рівні все ще бракує деталізованих підзаконних актів щодо стандартизованого захисту саме електронних публічних послуг. Існуючі стандарти більше орієнтовані на захист інформації в інформаційно-телекомунікаційних системах, ніж на веб-портали та хмарні сервіси, які використовуються для електронного урядування. Також потребує посилення нормативний контроль за кібергігієною державних службовців та користувачів електронних сервісів.

Окремою проблемою є відсутність обов'язкових аудитів безпеки нових цифрових сервісів перед їх запуском, зараз такі аудити проводяться фрагментарно. Хоча Закон України «Про основні засади забезпечення кібербезпеки України» чітко окреслює розподіл відповідальності між суб'єктами у сфері кібербезпеки, він у меншій мірі конкретизує механізми

практичної реалізації захисту кожного окремого електронного сервісу. Заповнення цих прогалин - через стандартизацію кіберзахисту публічних е-сервісів - залишається на порядку денному.

До недавна в Україні був відсутній чіткий законодавчий механізм щодо використання хмарних технологій державними органами. Це створювало правову невизначеність. Державні установи остерігались переносити дані у хмару через упередження порушити режим охорони інформації, а приватні провайдери не мали зрозумілих вимог для надання послуг уряду. Ситуація змінилася у 2022 році, коли було ухвалено Закон України «Про хмарні послуги» [26]. Цей закон визначив такі ключові терміни, як хмарний сервіс, провайдер хмарних послуг тощо, та встановив правові засади використання хмарних технологій у публічному секторі. Зокрема, він запровадив принцип «cloud first» для державних органів, окреслив вимоги до провайдерів, які працюють з державними замовниками, та зобов'язав забезпечувати належний захист даних при їх обробці у хмарі. Важливо, що закон дозволив державним інформаційним ресурсам розміщуватися у хмарних дата-центрах при дотриманні вимог безпеки, що стало критичним під час війни, коли постало питання географічного резервування даних.

Проте попереду лишається завдання імплементації, пов'язане з тим, що державні органи мають адаптувати свої ІТ-системи до нових правил, навчитися укладати ефективні контракти з хмарними провайдерами та гарантувати кібербезпеку в умовах, коли дані фізично можуть зберігатися за межами відомчого центру обробки. Отже, ухвалення закону про хмарні послуги заповнило значну прогалину, але практичне впровадження цього інструменту ще триває.

Сфера ШІ є відносно новою і національне законодавство тут перебуває в початковій стадії формування. На сьогодні відсутній спеціальний закон, який би регулював розробку і застосування систем штучного інтелекту в Україні, натомість існують лише політичні документи та рекомендації. У 2020 році Кабінет Міністрів схвалив Концепцію розвитку штучного інтелекту в Україні,

що визначає стратегічні цілі та принципи, пріоритет безпеки, етичність, сприяння інноваціям. Однак ця Концепція має більше декларативний характер і не встановлює обов'язкових норм для суб'єктів ринку чи державних органів. Практика впровадження ШІ наразі регулюється загальними нормами. Наприклад, законодавством про захист персональних даних, щодо біометричної ідентифікації, чи нормами цивільного права, щодо відповідальності за шкоду від програмних продуктів. У ЄС тим часом завершується розробка спеціального Акту про штучний інтелект, який класифікує ШІ-системи за рівнями ризику і встановлює вимоги до кожної категорії. Україна як держава-кандидат до ЄС буде зобов'язана імплементувати ці правила. Отже, наразі головна прогалина - це відсутність нормативної бази для оцінки безпечності та сертифікації систем ШІ. Питання відповідальності за прийняття рішень ШІ, прозорості алгоритмів, недопущення дискримінації алгоритмами - все це залишається поза межами спеціального регулювання. Експерти звертають увагу, що вже зараз варто адаптувати українську нормативну базу до підходів ЄС, наприклад, запроваджувати вимоги щодо оцінки впливу високоризикових систем ШІ та етичних принципів їх використання. В перспективі прийняття рамкового закону про штучний інтелект в Україні є необхідним кроком для забезпечення балансу між інноваціями і безпекою та правами людини.

Електронна ідентифікація громадян, ключ до доступу до електронниз послуг, також не до кінця цілісно врегульована. З одного боку, завдяки Закону України «Про електронні довірчі послуги» запроваджено BankID НБУ та інші засоби віддаленої ідентифікації, з іншого - відсутній єдиний закон, що визначав би державну політику у сфері цифрової ідентичності. На сучасному етапі в Україні функціонує декілька механізмів електронної ідентифікації, а саме система банківської дистанційної ідентифікації, яка дозволяє громадянам підтверджувати свою особу в державних порталах через банк, технологія SIM-карток з вбудованим кваліфікованим підписом, запущена у 2018 році, державний портал «Дія» - не є самостійним засобом ідентифікації, але інтегрує

існуючі (BankID, електронний підпис, MobileID). Україна однією з перших країн узаконила цифровий паспорт. Проте, хоча цифрові документи визнані, єдиної системи цифрової ідентифікації поки немає - громадяни використовують різні засоби, а єдиний реєстр електронних ідентифікацій не створений. У сфері електронної ідентифікації прогалина полягає не стільки в відсутності засобів, скільки у відсутності комплексної архітектури цифрової ідентичності. Потрібен єдиний підхід, що поєднає різні механізми та забезпечить їх взаємну сумісність і рівень довіри.

Європейський Союз наразі запроваджує систему Єдиної цифрової ідентичності (European Digital Identity Wallet) [81], і Україні доцільно узгодити свої кроки з цією ініціативою. Законодавчо варто врегулювати питання використання біометричних даних для онлайн-верифікації, порядок функціонування єдиної системи електронної ідентифікації, це означає фактично - надати BankID статус національної системи eID та визначити рівні довіри до різних методів аутентифікації. Наразі такі положення частково містяться в підзаконних актах і в згаданому законі про довірчі послуги, але цілісної картини на рівні закону немає. Результати аналізу, здійсненого в даному розділі підсумовано в таблиці 2.3.

Таблиця 2. 3.Структура нормативно-правового забезпечення електронного урядування в Україні в контексті інформаційної безпеки

Сфера нормативного забезпечення	Основні нормативно-правові акти	Проблеми та прогалини	Перспективні напрями розвитку
Стратегічні акти розвитку інформаційного суспільства	Закон «Про Національну програму інформатизації», Концепція розвитку цифрової економіки, Стратегія цифрової трансформації	Необхідність оновлення з огляду на сучасні реалії та війну	Оновлення стратегій, гармонізація з європейськими нормами
Інформаційна та кібербезпека	Доктрина інформаційної безпеки, Закони «Про основи національної безпеки», «Про національну безпеку», «Про кібербезпеку»	Потреба у деталізації вимог до кіберзахисту сервісів	Розвиток стандартів кіберзахисту, створення національної системи кібербезпеки
Захист персональних даних	Закон «Про захист персональних даних»	Недостатня гармонізація з GDPR	Повна імплементація GDPR, створення незалежного органу захисту даних
Хмарні технології	Закон «Про хмарні послуги»	Потреба в практичному впровадженні закону	Імплементація та адаптація державних систем до хмарних сервісів
Цифрова ідентифікація	Регулювання BankID, MobileID, цифрових документів, портал «Дія»	Відсутність єдиної законодавчої системи ідентифікації	Створення єдиної системи електронної ідентифікації відповідно до європейських стандартів
Технології штучного інтелекту (ШІ)	Концепція розвитку ШІ	Відсутність спеціального закону	Прийняття рамкового закону, адаптація до норм ЄС
Інформаційні відносини та відкритість	Закони України «Про інформацію», «Про доступ до публічної інформації»	–	–
Електронні послуги та документообіг	Закони України «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги»	–	–

Джерело: систематизовано і побудовано автором

Законодавче поле інформаційної безпеки електронного урядування потребує подальшого розвитку. В сфері персональних даних іде оновлення закону згідно з GDPR, у кіберзахисті - потрібна деталізація вимог до безпеки електронних сервісів, у хмарних технологіях важливо впровадити прийнятий закон на практиці, у штучному інтелекті необхідно розробити нові правила, а у цифровій ідентифікації звести окремі рішення в єдину систему. Вирішення цих завдань вимагатиме як адаптації нормативних актів, так і інституційних зусиль, що розглядається у наступному розділі.

Для подальшого розвитку нормативно-правового забезпечення електронного урядування в Україні доцільним є продовження гармонізації законів з правовим полем ЄС, особливо в сферах захисту даних, електронної ідентифікації, регулювання ШІ. Це означає необхідність ухвалити такі відсутні правові акти як рамковий закон про штучний інтелект, оновлену стратегію інформаційної безпеки з урахуванням гібридних загроз, забезпечити належне виконання вже прийнятих норм через підзаконні акти та інституційну спроможність. Також посилити відповідальність за кіберінциденти і порушення у сфері електронного урядування.

Реалізація законодавства залежить від інституційного забезпечення електронного урядування. В Україні сформовано розгалужену інституційну структуру, до якої входять органи, відповідальні за цифрову трансформацію, кібербезпеку, захист інформації та боротьбу з кіберзлочинністю. Ключовими суб’єктами виступають Міністерство цифрової трансформації України, Державна служба спеціального зв’язку та захисту інформації України, Національний координаційний центр кібербезпеки при РНБО, Національна поліція (кіберполіція) та інші (СБУ, НБУ тощо).

Міністерство цифрової трансформації України (Мінцифри) є головним органом у системі виконавчої влади, що формує і реалізує державну політику у сферах цифровізації, розвитку цифрової економіки, електронного урядування та суміжних напрямів. Згідно з Положенням про Міністерство [60], Мінцифри відповідає за впровадження електронного документообігу,

розвиток відкритих даних, національних електронних інформаційних ресурсів, електронних послуг, електронної ідентифікації та довірчих послуг, цифрових навичок громадян тощо. Таким чином, цей орган фактично координує усі проекти цифрової держави - від порталу «Дія» до розвитку широкосмугового доступу до мережі Інтернет і режиму «Дія Сіті» для IT-індустрії.

Діяльність Мінцифри вирізняється високою динамічністю та проактивним підходом. За короткий час міністерство запустило понад 100 електронних послуг на єдиному порталі «Дія», впровадило мобільний застосунок з цифровими документами, який став популярним серед громадян (понад 18 млн. користувачів), а також ініціювало проекти «Дія.Освіта» (цифрова грамотність) і «Дія.Бізнес» (підтримка підприємців).

Стосовно транспарентності, Мінцифри демонструє відкритість у своїй роботі. Воно активно висвітлює прогрес цифровізації, публікує звіти і статистику (на онлайн-панелі «Дія.Статистика» відображаються дані про користування е-послугами), залучає громадськість через обговорення нормативних актів на сайті. В міжнародних рейтингах електронного уряду Україна завдяки зусиллям Мінцифри покращила позиції. Це свідчить про ефективність міністерства у впровадженні цифрових реформ навіть в умовах війни. Водночас викликом для Мінцифри залишається інтеграція вимог інформаційної безпеки у всі цифрові проекти - для цього воно тісно співпрацює з Держспецзв'язку та РНБО. Загалом, Мінцифри стало рушійною силою цифрової трансформації, забезпечивши політичну пріоритетність цього напряму і консолідувавши зусилля різних органів.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) є основним суб'єктом, відповідальним за кіберзахист та урядовий зв'язок. Згідно із законодавством, Адміністрація Держспецзв'язку формує та реалізує державну політику у сфері кіберзахисту і відповідає за захист державних інформаційних ресурсів та критичної інформаційної інфраструктури. Тобто, цей орган визначає стандарти і вимоги безпеки для

державних інформаційних систем, проводить атестацію комплексних систем захисту, контролює стан захищеності державних електронних реєстрів, телекомунікаційних мереж, об'єктів критичної інфраструктури.

До структури Держспецзв'язку входять Адміністрація з департаментами кіберзахисту, технічного контролю тощо. Підпорядкованими установами є Державний центр кіберзахисту, Державний центр захисту інформаційно-телекомунікаційних систем, навчальні та наукові установи. Також при Держспецзв'язку діє урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка цілодобово здійснює моніторинг кіберінцидентів та координує реагування. Під час воєнного стану роль Держспецзв'язку зросла, фахівці спільно з СБУ та НБУ відбивали потужні кібератаки на банківський сектор, енергетику, держоргани; здійснювали міграцію урядових даних на хмарні сервіси; впровадили національний роумінг між мобільними операторами, щоб забезпечити зв'язок громадянам при пошкодженні веж.

В контексті координації, Держспецзв'язок тісно співпрацює з РНБО та її Координаційним центром кібербезпеки, а також з Мінцифри. Між Мінцифри та Держспецзв'язком є певний розподіл функцій. Перше відповідає за розвиток електронних сервісів, друге - за їх безпеку. Історично між цими органами виникали дублювання в частині питання електронних підписів. Наразі, Мінцифри є головним у політиці цифровізації, а Держспецзв'язок - у політиці кібербезпеки. Такий дуалізм вимагає постійної координації, щоб безпекові вимоги не гальмували цифрові інновації, і навпаки - щоб впровадження нових сервісів не створювало ризиків. Координація здійснюється, зокрема, через засідання РНБО і профільні робочі групи.

Для міжвідомчої координації зусиль було створено Національний координаційний центр кібербезпеки як робочий орган РНБО України. Його головою є Секретар РНБО, а до складу входять представники ключових суб'єктів кібербезпеки - СБУ, Служби зовнішньої розвідки, Міноборони/Генштабу, Нацполіції, НБУ, Держспецзв'язку та інші. Основним завданням цього органу є координація діяльності суб'єктів сектору безпеки і

оборони під час реалізації Стратегії кібербезпеки України та підвищення ефективності управління у сфері кібербезпеки. Центр збирає та аналізує дані про кіберінциденти, готує огляди стану кібербезпеки, які становлять базис рішень РНБО. З точки зору ефективності, створення даного центру суттєво покращило міжвідомчу співпрацю. Якщо раніше спостерігались розрізнені дії, то зараз є механізм узгодження і спільного реагування. Однак, спостерігається дублювання функцій різними державними структурами у сфері забезпечення інформаційної безпеки в електронному урядуванні. Так, СБУ та кіберполіція можуть розслідувати схожі кіберзлочини, або конкуренція за повноваження.

Підрозділ, відповідальний за протидію кіберзлочинності, функціонує в системі МВС після реформи колишнього управління боротьби з кіберзлочинами. Кіберполіція є міжрегіональним органом кримінальної поліції, що забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинами та проводить оперативно-розшукову діяльність у цій сфері. Спеціалізація кіберполіції полягає у виявленні, попередженні, припиненні та розкритті злочинів, пов’язаних із використанням комп’ютерних мереж і систем. Це охоплює широкий спектр таких правопорушень, як хакерські атаки на інформаційні системи, несанкціоноване втручання в роботу комп’ютерів і мереж, поширення шкідливого програмного забезпечення, крадіжки коштів через онлайн-шахрайства, фішинг, незаконний обіг персональних даних, платіжні афери тощо.

Загальна оцінка інституційної системи електронного урядування України є неоднозначною. З одного боку, наявні основні елементи та механізми координації, визначено відповідальних за всі напрямки, створено координаційний центр, запроваджено міжвідомчий обмін інформацією. З іншого боку, проблеми все ще мають місце, іноді бракує оперативності в ухваленні рішень (через бюрократичні процедури між відомствами), не повністю усунуто дублювання функцій в питаннях стандартів для ІТ-систем, є дефіцит висококваліфікованих кадрів, особливо в регіонах.

Інституційна модель в Україні еволюціонує в бік все більшої злагодженості. Законодавче закріплення повноважень створило основу, а практика спільної протидії кібервикликам під час війни зміцнила неформальні зв'язки між відомствами. Подальше вдосконалення цієї системи може відбутися шляхом чіткого розмежування компетенцій і уникнення дублювання, впровадження сучасних інструментів обміну даними між органами, підвищення прозорості для громадськості та продовження міжнародної інтеграції.

Не менш важливою є активна участь України у міжнародних ініціативах та обмінах досвідом - як на рівні експертів, так і на рівні укладення угод про взаємне визнання електронних довірчих послуг, спільну боротьбу з кіберзлочинністю тощо. Актуальним завданням є трансформація цієї бази у цілісну, сучасну і гнучку систему, здатну відповісти як на можливості технологічного прогресу, так і на виклики гібридної війни. Наукові дослідження і експертні напрацювання вказують на необхідність поєднання інновацій та безпеки в правовому регулюванні - лише за такої умови електронне урядування стане надійним інструментом зміцнення державності та сервісної взаємодії між владою і громадянами в цифрову епоху.

Висновки до розділу 2

У другому розділі дисертаційної роботи було здійснено комплексний аналіз сучасного стану системи електронного урядування в Україні, особливу увагу приділено аспектам забезпечення інформаційної безпеки. Проведене дослідження дозволило сформулювати низку теоретично значущих та практично спрямованих висновків.

1. За результатами оцінювання сучасного стану електронного урядування в Україні встановлено, що воно характеризується активним процесом цифровізації публічних послуг та розвитком інноваційних цифрових платформ, серед яких найвагомішим є впровадження системи «Дія». Це

сприяло суттєвому підвищенню якості та доступності державних послуг і поліпшенню взаємодії між державою та громадянами. Однак, незважаючи на помітний прогрес, впровадження цифрових сервісів характеризується нерівномірністю, особливо в регіональному розрізі, що свідчить про необхідність посилення інституційної підтримки, фінансування та організаційних заходів з боку держави.

2. Аналіз загроз та ризиків інформаційній безпеці в електронному урядуванні України дозволив визначити їх основні типи. Загрози було класифіковано за джерелами походження на внутрішні та зовнішні. До внутрішніх загроз віднесено недостатню кваліфікацію персоналу, низький рівень кібергігієни серед працівників державних установ, організаційні помилки та технічні недоліки, що створюють умови для вразливості інформаційних систем. Серед зовнішніх загроз найбільш значущими визначено активну діяльність організованих кіберзлочинних груп, кібершпигунство та масовані інформаційні атаки з боку інших держав, передусім Російської Федерації. Особливо гостро проблема зовнішніх кіберзагроз постала після повномасштабного військового вторгнення 2022 року, коли суттєво зросла кількість цілеспрямованих кібератак на державні інформаційні ресурси України.

3. Встановлено, що нормативно-правове забезпечення електронного урядування в Україні сформоване на достатньому рівні, однак аналіз засвідчив наявність суттєвих прогалин, які потребують усунення. Виявлені проблеми стосуються, передусім, недостатнього регулювання питань захисту персональних даних у відповідності до європейських стандартів GDPR, кібербезпеки цифрових державних сервісів, правового регулювання застосування хмарних технологій та штучного інтелекту. Хоча базові закони, такі як «Про інформацію», «Про доступ до публічної інформації», «Про електронні документи та електронний документообіг», закладають фундаментальні основи для розвитку цифрових процесів у державному

управлінні, їх регулярне оновлення та гармонізація з міжнародними стандартами є нагальною потребою.

4. З’ясовано, що належна реалізація законодавчих норм щодо забезпечення інформаційної безпеки електронного урядування потребує суттєвого посилення інституційної спроможності відповідальних державних органів. Незважаючи на визначені законодавством повноваження Міністерства цифрової трансформації України та Державної служби спеціального звя’зку та захисту інформації України, практичне виконання встановлених норм стримується недостатністю координації між відомствами, нерегулярністю проведення аудитів кібербезпеки та недостатнім рівнем цифрової грамотності державних службовців. Отже, критично необхідним є запровадження системного підходу до підготовки персоналу та постійний контроль за виконанням визначених нормативних вимог.

5. Доведено, що подальший ефективний розвиток електронного урядування в Україні, особливо в умовах сучасних викликів інформаційній безпеці, вимагає комплексного підходу. Такий підхід передбачає, зокрема, оновлення та системне удосконалення нормативно-правової бази, підвищення інституційної спроможності відповідальних органів, впровадження сучасних технологій захисту інформації та розвиток цифрових компетенцій як державних службовців, так і пересічних громадян. Саме такий підхід здатний забезпечити високий рівень інформаційної безпеки в електронному урядуванні та створити передумови для подальшої цифровізації публічного управління в Україні.

Основні положення розділу дисертаційної роботи відображені в працях автора [36, 123]

РОЗДІЛ 3
ПРОПОЗИЦІЇ ЩОДО РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Стратегічні напрями розвитку електронного урядування в контексті забезпечення інформаційної безпеки

На основі проведеної оцінки сучасного стану електронного урядування в Україні та аналізу загроз інформаційній безпеці, очевидно, що подальший розвиток цифрових державних послуг має здійснюватися з урахуванням факторів безпеки і довіри. Зокрема, повномасштабна війна різко загострила вразливості, кібератаки агресора спрямовані на реєстри, платформи й комунікації, прагнучи підірвати довіру громадян до існуючої системи електронного урядування [52, 64]. В таких умовах забезпечення інформаційної безпеки стало критично важливим для безперервності державного управління навіть у кризових ситуаціях [52, 64]. Одночасно держава досягла значного прогресу у цифровізації (64% українців уже користуються онлайн-послугами [69]), що вимагає належного захисту даних та приватності користувачів. Нормативно-правова база також розвивається. Діють закони про кібербезпеку, захист персональних даних, електронну ідентифікацію, хмарні послуги тощо, ухвалено Стратегію кібербезпеки України [29]. Втім, виникає потреба їх актуалізації та гармонізації із сучасними європейськими стандартами (GDPR, NIS2, AI Act тощо) для належного захисту інформації.

Як ми зазначали у першому розділі, електронне урядування слід розглядати як інструмент забезпечення інформаційної безпеки та впровадження сучасних форм управління відповідно до національних і міжнародних норм. Відтак, стратегічні підходи до розвитку електронного урядування мають інтегрувати безпекову складову на всіх етапах, розвиватися в концепції цифрового уряду. За визначенням ООН, цифровий уряд - це

«екосистема взаємопов’язаних інституцій, процесів і технологій, що функціонують у цифровому середовищі, керуючись принципами орієнтації на користувача, інклюзивності, довіри та безпеки» [98]. Тому підвищення рівня довіри громадян через забезпечення інформаційної безпеки є ключовою умовою успішної цифрової трансформації державної влади.

Ми вважаємо за доцільне структурувати стратегічні напрями розвитку системи електронного урядування за часовими горизонтами. Доцільність розробки стратегічних напрямів розвитку системи електронного урядування в Україні саме за часовими горизонтами випливає з необхідності формування послідовної, чітко структурованої і реалістичної політики, яка здатна комплексно вирішити сучасні проблеми й виклики інформаційної безпеки. Застосування підходу, заснованого на поділі стратегічних напрямів на коротко-, середньо- та довгострокову перспективи, дозволяє розподілити цілі й завдання з урахуванням їх пріоритетності, ресурсної забезпеченості та готовності інституційної структури державного управління до їх реалізації.

Короткострокові заходи (1-2 роки) спрямовані на вирішення найгостріших проблем та оперативне реагування на найбільш нагальні виклики, пов’язані, зокрема, з кібербезпекою і впровадженням мінімально необхідних регуляторних змін. Ці заходи закладають основу для подальшого розвитку, сприяючи формуванню довіри до електронних сервісів серед громадян і бізнесу.

Середньострокова перспектива (3-5 років) орієнтована на комплексні реформи, впровадження новітніх технологій та законодавчих ініціатив, що вимагають більшого часу для реалізації. На цьому етапі здійснюється системне узгодження нормативних актів із міжнародними стандартами та європейським законодавством, розгортається масштабна інституційна перебудова, формується єдина архітектура цифрових державних послуг з вбудованою системою інформаційною безпеки. Саме цей період є критично важливим для зміцнення довіри населення та досягнення суттєвих результатів у сфері цифровізації.

Довгострокова перспектива (понад 5 років) враховує стратегічні виклики та технологічні тренди, які неможливо реалізувати швидко через потребу значних інвестицій, формування нової інфраструктури та глибоких змін суспільної свідомості й культури користування цифровими технологіями. Саме тут закладається фундамент стійкої системи інформаційної безпеки, реалізуються масштабні трансформації, що дозволяють Україні інтегруватися у глобальний цифровий простір. Розподіл стратегічних напрямів за часовими горизонтами є методологічно обґрунтованим, оскільки забезпечує послідовність та узгодженість у реалізації цілей електронного урядування, дозволяє гнучко реагувати на нові виклики та можливості, а також визначати чіткі критерії ефективності й відповідальності за результати на кожному етапі розвитку (рис.3.1).

В короткостроковій перспективі, в найближчі 1-2 роки, слід розробити та затвердити оновлену національну стратегію розвитку електронного урядування, де інформаційна безпека визначається як інтегральна складова всіх цифрових проєктів, а не допоміжна функція. Важливо закласти принцип «security by design», що означає безпека з етапу планування та дизайну сервісів [77]. Досвід таких країн як Сінгапур, Данія демонструє, що наявність стратегії інформаційної безпеки, узгодженої з політикою електронного урядування, є одним з ключових факторів успіху у забезпеченні інформаційної безпеки [77]. Тому Україна має синхронізувати виконання Стратегії кібербезпеки та заходів цифрової трансформації. Зокрема, вже ухвалений План реалізації Стратегії кібербезпеки (2023-2024 роки) потребує належного ресурсного забезпечення, щоб впровадити нові стандарти захисту інформації в органах влади [59, 64].

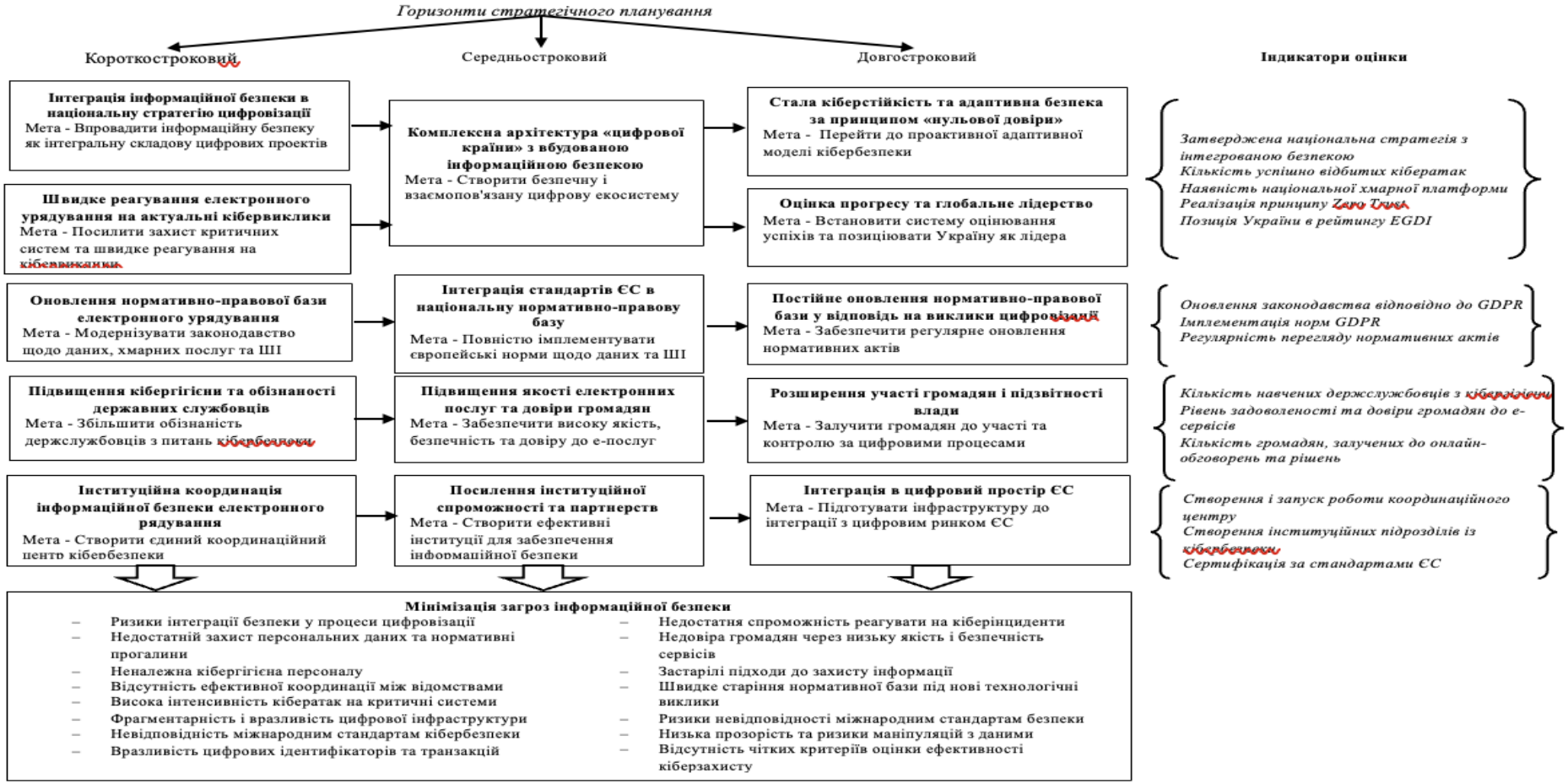


Рисунок 3.1. Модель стратегічного планування розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки

Джерело: розроблено автором

Протягом короткострокового періоду необхідно модернізувати законодавство для усунення найбільш критичних прогалин. Передусім це стосується захисту персональних даних. Так, Закон України «Про захист персональних даних» [18] слід привести у відповідність до Загального регламенту захисту даних ЄС (GDPR) [84]. Крім того, слід імплементувати Закон України «Про хмарні послуг» від 2022 року на практиці, розробивши підзаконні акти щодо стандартів захисту даних у державних хмарах. Паралельно необхідно закласти основи правового регулювання у сфері штучного інтелекту. Розробити рамковий закон щодо етичного і безпечного використання штучного інтелекту в державному секторі. Враховуючи, що лише близько 44% країн світу мають стратегії з розвитку хмарних технологій, а 42% - політики щодо штучного інтелекту [114]. Гармонізація з європейськими стандартами (регуляції ЄС щодо цифрових послуг, даних та ШІ) не лише підвищить безпеку обробки даних, а й зміцнить довіру міжнародних партнерів до українських електроних сервісів.

Людський фактор лишається одним з найуразливіших аспектів інформаційної безпеки, тому в короткостроковій перспективі варто зосередитися на навчанні та підвищенні кваліфікації персоналу. Необхідно запровадити програми обов'язкового навчання державних службовців основам кібергігієни, управління цифровими ризиками, безпечної роботи з даними. Досвід провідних країн свідчить, що рівень цифрової грамотності державних службовців прямо впливає на стійкість електронного урядування [114]. Наприклад, у Сінгапурі та Канаді реалізуються масштабні курси кібергігієни для державних працівників і населення [114]. За даними опитування ПРООН, майже третина громадян не звертається до електронних сервісів через відсутність інформації або навичок [110].

На особливу увагу заслуговує інституційна координація кібербезпеки електронного урядування в короткостроковій перспективі. В найближчі роки доцільно створити постійнодіючий міжвідомчий координаційний орган з

питань цифрової безпеки та довіри. Його задачами мають стати моніторинг кіберзагроз, реагування на інциденти, розробка стандартів безпеки для державних ІТ-систем та узгодження дій різних відомств. Корисним є досвід Естонії, де Агентство інформаційних систем виконує роль центру кіберзахисту держави та координує мережеву безпеку у всьому публічному секторі [105]. Україна вже має окремі елементи такої структури, наприклад, Головний центр спеціального контролю РНБО та команди CERT-UA. Проте бракує єдиного «контуру» управління інформаційною безпекою. Тому пропонується інституційно об'єднати зусилля Міністерства цифрової трансформації, Держспецзв'язку, СБУ та НБУ під спільним координуючим органом, можливо, на базі Національного координаційного центру кібербезпеки при РНБО. Подібний орган буде здатен забезпечити швидкий обмін інформацією про загрози та розробці цілісної політики захисту для всіх державних інформаційних ресурсів.

З огляду на рекордну інтенсивність атак останніх років, у короткостроковій перспективі пріоритетом має стати посилений захист найбільш критичних систем. Потрібно впровадити багатофакторну автентифікацію та сучасні засоби шифрування у всіх держустановах, сегментувати мережі та резервувати ключові державні реєстри на випадок атак. Важливо налагодити резервні канали зв'язку та живлення для порталів на кшталт «Дія», щоб забезпечити їх безперебійну роботу навіть за умов надзвичайних ситуацій. Одночасно слід розгорнути систему регулярного аудиту безпеки державних електронних сервісів за участю «етичних хакерів» та виправлення виявлених вразливостей. Ці кроки створять фундамент для подальших, більш масштабних трансформацій.

На середньостроковому горизонті в 3-5 років стратегічною метою є побудова цілісної цифрової екосистеми уряду, де всі компоненти, від реєстрів до сервісних платформ, взаємопов'язані та захищені за єдиними стандартами. Це передбачає розгортання національної хмарної інфраструктури для державних органів з високим рівнем захисту (сертифікація за стандартами ISO

27001 [88] тощо) і перенесення критичних систем у захищені дата-центри. Має бути забезпечена повна інтероперабельність між різними реєстрами та службами з чітким контролем доступу та протоколами обміну даними, що унеможливлюють несанкціонований витік. Принцип єдиного входу та архітектура «нульової довіри» («zero trust») повинні стати нормою. Це означає, що кожен запит до державної інформаційної системи перевіряється і кожна підмережа автоматично вважається такою, що не має достатнього захисту [114]. Подібні підходи вже впроваджуються країнами-лідерами. Так, у Південній Кореї стратегія «нульової довіри» закладає основу безпечної цифрової інфраструктури, а уряд Сінгапуру реалізував «Government Zero Trust Architecture» як стандарт для всіх відомств [114]. Для України важливо завершити перехід від розрізнених ІТ-рішень до єдиної національної платформи цифрового урядування («держава в смартфоні»), архітектурно захищеної від кіберзагроз.

У середньостроковій перспективі необхідно здійснити повноцінну імплементацію оновленої нормативної бази. Протягом найближчих 3-5 років Україна повинна запровадити сучасне законодавство про захист персональних даних гармонізоване з GDPR та створити дієвий незалежний орган з нагляду за приватністю. Також необхідно прийняти та реалізувати національну Стратегію розвитку штучного інтелекту на основі Концепції [40], узгоджену з підходом ЄС до етичного штучного інтелекту. В ЄС у 2024 році погоджено Акт про штучний інтелект, що запроваджує ризик-орієнтоване регулювання ШІ [40]. Україна має використати цей досвід для власного регулювання задля того, щоб технології штучного інтелекту застосовувалися безпечно і задля розвитку суспільства. Окрім того, слід долучитися до європейських ініціатив у сфері кібербезпеки, імплементації директиви NIS2 щодо захисту критичної інфраструктури, стандартів кібергігієни для органів влади тощо. Синхронізація українських норм із європейськими буде важливою і з огляду на перспективу членства в ЄС, і з позиції довіри. Тому у середньостроковій стратегії Україні слід закріпити принципи цифрових прав людини,

інформаційної безпеки та суверенітету даних, синхронізовані з європейськими.

Також увагу необхідно приділити розвитку системи електронної ідентичності та довірчих послуг. Закон «Про електронну ідентифікацію та електронні довірчі послуги» вже заклав основу [17]. На сучасному етапі слід забезпечити її реалізацію на практиці. Зокрема, потрібно розширити функціонал платформи «Дія» як єдиного цифрового посвідчення особи, інтегрувати нові методи eID (Mobile ID, Smart-ID тощо) та гарантувати взаємне визнання української електронної ідентифікації з іноземними державами. Доцільно впровадити національну програму Digital ID для всіх, аби кожен громадянин мав захищений засіб електронної автентифікації для доступу до держпослуг.

У ЄС набирає обертів проєкт European Digital Identity Wallet (цифровий гаманець ідентифікації) [114]. Україні варто приєднатися до пілотних проєктів у цій сфері з метою досягненя повної сумісності українських ідентифікаційних сервісів з європейськими. Розвиток цифрової ідентичності також пов’язаний із розбудовою інфраструктури електронного підпису, печатки, часових міток, що гарантують юридичну значимість електронних документів. Ці елементи довірчих послуг мають стати звичним інструментом до 2028-2029 років, забезпечуючи і зручність, і захищеність онлайн-взаємодії з державою.

Ще одним середньостроковим стратегічним напрямом розвитку має стати вихід новостворених інституцій кібербезпеки на повну ефективність. Координаційний центр, який ми зазначали раніше як стратегічний пріоритет у короткостроковій перспективі, має напрацювати власні аналітичні спроможності, систему раннього попередження загроз інформаційній безпеці та відповідні протоколи реагування. Державні установи повинні запровадити посади відповідальних за інформаційну безпеку, які взаємодіятимуть із центром. Також варто налагодити державно-приватне партнерство у сфері забезпечення інформаційної безпеки залучати вітчизняні компанії й стартапи до розробки рішень для безпеки електронного урядування, проводити спільні

навчання і обмін інформацією про загрози. К 2030 року Україна може створити консорціум за участі державних органів, ІТ-компаній та академічних установ для інновацій у сфері кібербезпеки, аналогічно до ізраїльських або естонських моделей.

Іншим напрямом інституційного розвитку є регіональний рівень, доцільно сформувати у кожній області підрозділи або центри компетенцій з цифрового розвитку та інформаційної безпеки, аби підвищити спроможність громад у захисті своїх інформаційних ресурсів.

Як ми зазначали раніше, цифровий уряд, насамперед, характеризується підвищенням якості електронних послуг та довіри громадян. Держава повинна продемонструвати громадянам відчутні вигоди від цифровізації, що відображаються в таких індикаторах як економія часу, прозорість, відсутність корупції при гарантованій безпеці даних. Для цього необхідно забезпечити високу надійність і зручність сервісів, скоротити випадки збоїв, технічних помилок, реалізувати користувацький інтерфейс з урахуванням потреб людей з різними можливостями. У середньостроковій перспективі слід впровадити постійно діючі платформи електронної участі, де громадяни зможуть обговорювати проєкти рішень, контролювати бюджети, повідомляти про проблеми. На середньостроковому етапі Україна повинна не лише розширити перелік цифрових послуг, але й забезпечити їх стале функціонування та високий кредит довіри з боку суспільства.

У довгостроковому вимірі стратегічною метою є перетворення інформаційної безпеки на невід'ємну властивість усіх процесів електронного урядування. Це означає перехід від реактивної моделі протидії загрозам до проактивної та адаптивної. Архітектура «нульової довіри», про яку ми зазначали раніше, має повністю реалізуватися в державних органах від центральних до локальних. Кожен новий пристрій або користувач, підключений до державної мережі, автоматично проходить багаторівневу перевірку автентичності та відповідності політикам безпеки. Використання штучного інтелекту для кіберзахисту повинно стати базисом для діагностики

в режимі реального часу аномалій трафіку. Вже зараз такі рішення впроваджені в Естонії та Південній Кореї і стали основою їхньої державної цифрової інфраструктури [114]. Через 5-7 років Україна також повинна мати розгорнуті системи Security Information and Event Management нового покоління з елементами штучного інтелекту, що інтегровані між усіма відомствами. Критично важливо забезпечити стійкість до новітніх загроз, які можуть постати у майбутньому, наприклад квантових атак.

У швидкозмінному цифровому середовищі держава повинна підтримувати актуальність своїх законів і політик. На довгострокову перспективу планується створення гнучкої нормативної системи, здатної швидко адаптуватися до появи нових технологій і загроз. Для цього необхідно запровадити механізми регулярного перегляду і оновлення цифрового законодавства. Наприклад, кожні 2-3 роки проводити аудит законів про електронні інформаційні відносини. Україна має інтегруватися в загальноєвропейський процес вироблення цифрових правил, брати участь у робочих групах ЄС з питань штучного інтелекту, кібербезпеки, захисту даних, щоб переймати кращі практики і готуватися до імплементації нових вимог ще до їх формального вступу в силу. Цілком логічним і закономірним є укладання нових міжнародних угод та стандартів, тож нормативно-правова база України має бути достатньо гнучкою для їх швидкого врахування. Це гарантія того, що розвиток таких технологій як ШІ, великі данні, інтернет речей та блокчейн, відбувається під належним правовим контролем, який збалансує інновації та інформаційну безпеку. Як зазначено у звітах ООН 2020-2024 років, розвиток цифрового уряду повинен супроводжуватися впровадженням принципів захисту прав, довіри та безпеки в усі проекти цифрової трансформації [112, 113, 114]. Це має знайти відображення і в українській нормативно-правовій базі, пріоритет прав громадян на приватність, безпеку даних і доступ до інформації закріплюється як незмінна основа незалежно від появи нових технологічних трендів.

В довгостроковій перспективі прогрес України в напрямі членства в ЄС відкриє можливості повноцінної участі у Єдиному цифровому ринку. Стратегічно важливо підготувати національну систему електронного урядування до такої інтеграції. Це означає, що українські електронні сервіси мають відповідати всім технічним і правовим вимогам ЄС щодо сумісності, безпеки та захисту даних. Зокрема, доцільно пройти добровільну сертифікацію за європейськими кіберстандартами - отримати відповідність критеріям EU Cybersecurity Certification Framework для державних послуг [107]. Україна має увійти до системи взаємного визнання електронних підписів та довірчих послуг ЄС, скориставшись можливостями, передбаченими регламентом eIDAS. У сфері електронної ідентичності завданням є приєднання до мережі European Digital Identity задля визнання українського цифрового паспорту «Дії» в країнах ЄС.

Довгостроковою ціллю також є забезпечення українським громадянам і бізнесу доступу до трансєвропейських цифрових послуг. Участь у публічних закупівлях інших країн через інтегровані системи, використання загальноєвропейських порталів охорони здоров'я, освіти тощо на рівні з громадянами ЄС. Це вимагає не лише нормативного, але й технічного узгодження. Використання відкритих європейських стандартів інтероперабельності, підключення до пан'європейських цифрових платформ. Тобто, у довгостроковій перспективі електронне урядування України має еволюціонувати з національної системи до органічної складової загальноєвропейського цифрового простору.

Довгострокове бачення розвитку електронного урядування включає утвердження моделі відносин держави і суспільства як «цифрової демократії». Впродовж наступних років слід досягти такого рівня залучення громадян, коли більшість важливих державних рішень обговорюються публічно онлайн, а громадський контроль стає невід'ємною частиною управлінських процесів. Довгострокова перспектива передбачає, що урядові дані відкриті максимально і регулярно оновлюються, щоб громадяни та бізнес могли їх вільно

використовувати для моніторингу та інновацій. Понад 90% країн світу вже публікують відкриті дані бюджету [114]. Країни-лідери світового рейтингу розвитку електронного урядування Данія, Південна Корея, Сінгапур вже перебувають на наступному етапі - це відкритість данних в режимі реального часу і впровадження елементів участі 2.0, що означає спільне прийняття рішень з громадянами онлайн. Такий ступінь прозорості та участь громадян запобігають зловживанням і підвищують легітимність влади, а отже, і довіру до електронних сервісів.

З метою оцінки прогресу в контексті довгострокових стратегічних напрямів розвитку електронного урядування доцільно запровадити систему оцінювання ефективності реалізації стратегічних цілей. Ключові показники можуть включати місце України у загальносвітовому рейтингу EGDI. Метою має стати входження до топ-20 країн. Рівень кіберготовності за National Cyber Security Index, зараз Україна перебуває на досить високій позиції - на 26-му місці із 160. Визначення частки громадян, які довіряють цифровим послугам, опитування мають фіксувати тенденцію до зростання цього показника. Як демонструє світовий досвід, забезпечення безпечного цифрового середовища прямо пропорційно впливає на зростання довіри громадян до держави [112, 113, 114]. У перспективі Україна теж зможе поділитися власним унікальним досвідом побудови цифрової держави під час війни, зробивши свій внесок у глобальні стандарти інформаційної безпеки і електронного врядування.

Стратегічні напрями, окреслені для короткострокового, середньострокового та довгострокового періодів, формують дорожню карту розвитку електронного урядування України з урахуванням пріоритетів інформаційної безпеки. Вони логічно випливають із виявлених проблем сучасного стану - вразливість реєстрів, недостатня довіра, фрагментарність нормативної бази та спрямовані на досягнення цілісного результату, а саме створення стійкої, захищеної та орієнтованої на громадян цифрової держави. Поєднання підвищення кіберстійкості, оновлення законодавства, розвитку цифрової ідентичності, інституційних реформ і гармонізації з європейськими

стандартами дозволить забезпечити баланс між інноваціями і безпекою. Як наслідок, зростатиме довіра суспільства до електронного урядування, що є фундаментом успішної цифрової трансформації.

Уряд країни визначає стратегічний напрям, але практична реалізація багатьох ініціатив залежить від спроможності регіонів адаптувати їх до своїх потреб. Держава спрямовує цифрові реформи «до низу», забезпечуючи єдність підходів і обмін найкращими практиками між центром та регіонами. Як наслідок, успіхи України у розвитку електронного уряду багато в чому залежать від прогресу кожного регіону. Цифровізація регіонів є обов'язковим елементом розвитку держави в цілому, регіони не просто виконують допоміжну роль, вони стали активними суб'єктами цифрових змін.

3.2. Удосконалення механізму розвиток електронного урядування на регіональному рівні

Регіони України відіграють ключову роль у цифровій трансформації державного управління, адже значна частина електронних послуг надається на місцевому рівні через органи місцевої влади та громади. Реформа децентралізації розширила повноваження громад, що створило передумови для активнішого впровадження цифрових рішень на місцях. Попри загальну позитивну динаміку, залишається проблема цифрового розриву між різними регіонами та соціальними групами.

Доступ до якісного інтернет-зв'язку та сучасних технологій суттєво різниться залежно від географії. У віддалених селах Карпа, на прифронтових територіях доступ до широкосмугового інтернету все ще обмежений, що знижує можливість користуватися електронними послугами на рівні з мешканцями міст. Війна проти України ще більше загострила проблеми нерівномірного доступу. У 2022 році через бойові дії і окупацію окремих територій тисячі громадян втратили доступ до інтернету та державних електронних сервісів. Збої живлення та руйнування мереж призвели до того,

що уряду довелося тимчасово зосередитися на відновленні базової інфраструктури та кібербезпеки замість розвитку нових цифрових послуг. Найбільше постраждали прифронтові області Донецька, Луганська, Херсонська, Запорізька, де фізичне пошкодження мережевого обладнання і відтік населення призвели до цифрової ізоляції багатьох громад. Водночас, інші відносно безпечні регіони продовжували модернізацію, що призвело до ситуації «різношвидкісної» цифровізації. Так, у центральних та західних областях громадяни швидко повернулися до онлайн-послуг через застосунок «Дія» у 2023-2024 роках [29], тоді як на прифронтовому півдні та сході України багато сервісів залишалися недоступними. До традиційних причин нерівномірності, географії, щільності населення, доходів, додались нові виклики безпеки. В результаті виникла потреба у спеціальних заходах цифрової інклюзії.

Україна за підтримки міжнародних партнерів впроваджує проєкти для скорочення цифрового розриву, а саме відкриваються безкоштовні цифрові хаби у селах, запускаються навчальні курси з цифрової грамотності для літніх людей, субсидіюється підключення віддалених громад до інтернету у т.ч. через супутникові технології, розгортати програми навчання для осіб похилого віку, цифровізувати школи, вирівнювати ціни на інтернет і забезпечити рівний інтернет-доступ у різних регіонах [29]. Поступово ці кроки дають ефект, дослідження показують [91], що за останнє десятиліття регіональний розрив за базовим доступом до інтернету скоротився - коефіцієнт варіації частки користувачів інтернету зменшився з 36,4% у 2010 році до 10,2% у 2019 році [29]. Втім, користування більш складними електронними сервісами як пряма взаємодія з органами державної влади онлайн досі суттєво варіюється між областями [29]. Це свідчить, що проблему нерівномірного доступу не вирішено остаточно, і вона потребує комплексної регіональної політики цифрової інклюзії.

Попри різні стартові умови, за останні роки всі області України розпочали шлях цифрової модернізації. Для оцінки прогресу Міністерство

цифрової трансформації запровадило Індекс цифрової трансформації регіонів, який комплексно вимірює досягнення кожної області. Цей рейтинг враховує дев'ять ключових аспектів розвитку цифровізації [29]:

- інституційна спроможність (наявність цифрових стратегій, підрозділів, фахівців у регіоні);
- розвиток інтернет-інфраструктури (покриття broadband, мобільний інтернет);
- розвиток центрів надання адмінпослуг - ЦНАП (число і якість ЦНАПів, їх цифровізація);
- впровадження режиму «без паперів» (перехід державних установ на електронний документообіг та електронні формати);
- цифрова освіта (доступність онлайн-освіти, цифрова грамотність населення);
- «візитівка» області (цифрова присутність, сучасний сайт ОДА, відкриті дані, електронні портали регіону);
- проникнення базових електронних послуг (рівень використання мешканцями ключових електронних послуг);
- галузева цифрова трансформація (впровадження ІТ-рішень у різних сферах, е-медицина, е-логістика, розумне місто тощо);
- індивідуальні інноваційні проєкти, які команда цифровізації реалізувала в цьому регіоні.

За результатами 2023 року лідери цифрової трансформації чітко окреслились (Додаток Г). До трійки найкращих областей увійшли Львівська, Дніпропетровська та Одеська області [29]. Ці регіони показали високі результати за всіма критеріями індексу завдяки ефективній роботі команд цифровізації та підтримці з боку місцевої влади. Зокрема, в трьох зазначених областях протягом 2023 року спільними зусиллями впроваджено 125 інноваційних цифрових проєктів. Багато з цих регіональних ініціатив стали зразковими і були поширені на інші області [29].

Одеська область демонструє показовий досвід регіональної цифрової модернізації. Наряду з технічними рішеннями було реалізовано низку цифрових сервісів для громадян. Запущено ШІ-асистент «Сталевий Дюк», що виступає віртуальним гідом та експертом для мешканців області, створено онлайн-платформу «Спільнота» для збору і систематизації потреб громад, відкрито Military Hub для підтримки військових стартапів, а також розгорнуто цифрову туристичну платформу для промоції регіону [29]. Такий комплексний підхід - від зміцнення інфраструктурної стійкості до запуску високотехнологічних проєктів - вивів Одеську область у лідери цифровізації.

Інші регіони-лідери теж мають успішні практики. Львівська область традиційно інвестує в ІТ-галузь і електронне урядування, тут діють численні стартапи, а Львів став одним із центрів розробки цифрових сервісів для громади - від електронних петицій до системи електронного квитка в транспорті. Дніпропетровська область сфокусована на впровадженні принципу «держави у смартфоні» на місцевому рівні. Область однією з перших повністю перейшла на електронний документообіг в обласній військовій адміністрації і районних адміністраціях, активно розвиває мережу ЦНАПів та електронні послуги для бізнесу [29].

Полтавська область, хоч і не перебуває у трійці лідерів за 2024 рік, але за підсумками 2023 року увійшла до топ-3 областей за індексом цифрової трансформації [29]. Сильними сторонами є розвиток ЦНАПів, реалізація політики безпаперової документації, увага до цифрової освіти.

Втім, поряд із позитивним досвідом існують проблемні приклади регіональної цифровізації. Найскладніша ситуація у регіонах, що опинилися в зоні бойових дій або довготривалої окупації. Луганська та Донецька області, частково непідконтрольні Україні з 2014 року, відставали в розвитку електронного урядування ще до повномасштабної війни, а після 2022 року їх цифрова інфраструктура зазнала катастрофічних втрат. Відповідно, показники по цих областях або не враховуються, або мінімальні.

Херсонська область у 2022 році пережила окупацію, було знищено сервери, викрадено обладнання, бази даних громад піддались ризику компрометації [91]. Після деокупації регіон фактично змушений будувати цифрове управління з початку. Чернігівська та Сумська області, які зазнали масштабних руйнувань інфраструктури на початку війни, також відстали за рядом цифрових показників у 2022 році.

Окрім військових факторів, на результати впливає й економічна спроможність. Такі промислові регіони як Дніпропетровський, Запорізький мали ресурси інвестувати в ІТ-рішення, натомість депресивні аграрні регіони часто не мали достатнього фінансування. Дослідження підтверджують зв'язок між економічним розвитком регіону та рівнем його цифровізації [29, 91].

Проблемними є й окремі міські громади, де відсутня політична воля до прозорості та цифрових змін, там і далі домінує паперова бюрократія, а впровадження електронних послуг гальмується. Достатньо показовим є те, що успішними можуть бути не лише великі міста, але й менші громади за умови правильної стратегії. Так, м. Стрий Львівської області, маючи населення близько 60 тис. осіб, увійшло до сотні найкращих цифрових громад України серед понад 1000 оцінених громад [29]. Це стало можливим завдяки прогресивному міському керівництву, яке впровадило елементи «Smart City», електронні кабінети мешканця, онлайн-сервіси ЖКГ тощо.

Інформаційна безпека в електронному урядуванні на рівні регіонів стала невід'ємною складовою загальної національної безпеки, особливо в умовах гібридної війни. Основні виклики регіональної інформаційної безпеки можна поділити на чотири групи. По-перше, недостатній захист мереж та сайтів місцевих органів влади через брак сучасних засобів кіберзахисту. Багато громад до війни не мали комплексних систем захисту (систем виявлення вторгнень, резервного копіювання даних тощо), що зробило їх вразливими. По-друге, людський фактор, частина кібератак стала можливою через низьку обізнаність співробітників на місцях - елементарне недотримання правил кібергігієни, фішингові листи, слабкі паролі. По-третє, не всі регіони

інтегровані в єдину державну систему моніторингу інцидентів, що ускладнює швидке реагування. Хоча на центральному рівні діє команда CERT-UA і створено Government Security Operations Center (SOC), на рівні областей подекуди бракує виділених команд реагування. По-четверте, війна змінила пріоритети, в розпал бойових дій 2022 року кібербезпека тимчасово відходила на другий план перед фізичним виживанням структур. Лише після стабілізації ситуації наприкінці 2022 - 2023 році більшість регіонів відновили роботу над посиленням кіберзахисту.

Попри ці виклики, Україна напрацьовує рішення для забезпечення інформаційної безпеки в електронному урядуванні на регіональному рівні. У кожній області призначено відповідальних за кібербезпеку в обласних адміністраціях, зазвичай це підрозділи захисту інформації при ІТ-відділах. Іншим нововведенням стала вимога резервування даних. Після випадків знищення серверів в зоні бойових дій, уряд зобов'язав критичні реєстри і бази даних дублювати в захищених дата-центрах у безпечних регіонах або в хмарних сервісах. Так, дані багатьох громад Донецької області зберігаються в хмарі Держспецзв'язку. Україна також розгорнула співпрацю з ЄС і НАТО щодо кібероборони. У лютому 2022 року, напередодні вторгнення, ЄС вперше активував свою команду швидкого кіберреагування для допомоги Україні [82]. Ці фахівці, спільно з українськими, відпрацьовували атаки і допомогли підготувати регіональні системи до нових загроз. Як результат, попри безпрецедентну хвилю кібератак, українська цифрова інфраструктура вистояла, а жодна критична база даних місцевого самоврядування не була знищена чи скомпрометована безповоротно.

Інституційна спроможність регіонів і громад - один з визначальних факторів успішної цифрової трансформації. Під цим розуміється наявність у місцевої влади компетентних кадрів, структур, фінансів та нормативної бази для реалізації цифрових змін. На практиці в Україні рівень інституційної готовності різниться. Якщо обласні державні адміністрації зазвичай мають ІТ-відділи та призначених уповноважених з питань цифрового розвитку, то у

багатьох невеликих громадах відповідальність за цифровізацію часто покладається на одну-дві особи, або взагалі поєднується з іншими обов'язками. Це створює ризики, що на місцях бракуватиме експертизи для впровадження складних проєктів.

Останні роки позначилися прогресом у розбудові інституційної спроможності на регіональному рівні. По-перше, завдяки зусиллям Міністерства цифрової трансформації практично в кожній громаді призначено цифрового лідера - уповноваженого з питань цифрового розвитку. Станом на кінець 2024 року таких локальних CDTO налічувалося вже понад дев'ятсот. Вони стали своєрідними «агентами змін», відповідальними за впровадження центральних ініціатив, таких як застосунок «Дія», реєстр адрес, електронний документообіг на рівні своїх міст і сіл. По-друге, для координації зусиль створено горизонтальні майданчики обміну досвідом. Це дозволяє виявити потреби на місцях і узгодити пріоритети цифровізації знизу вгору. По-третє, за підтримки донорів поліпшується матеріальна спроможність громад, так швейцарсько-українська програма EGAP [67] фінансує оновлення та відбудову ЦНАПів, впровадження нових онлайн-послуг, розвиток інфраструктури в пілотних громадах. До 2028 року основною метою є створення показових «цифрових громад», які стануть орієнтиром для інших.

Попри ці позитивні зрушення, залишається низка проблем інституційного характеру. Дослідження відзначають такі вузькі місця, як забюрократизованість комунікацій між різними рівнями влади, нестачу кваліфікованих IT-фахівців, особливо у сільських районах, обмеженість фінансування - місцеві бюджети часто не передбачають достатньо коштів на цифрові проєкти, недостатня залученість громадян, населення подекуди не використовує вже створені е-сервіси, через що місцева влада не відчуває запиту на їх розширення [43]. Також відзначається низький рівень популяризації успішних кейсів - позитивний досвід окремих міст не завжди відомий іншим громадам.

Для успішної цифрової трансформації критично важливим є налагоджена взаємодія між центральною владою та місцевими громадами. В Україні формується модель, за якої держава виступає стратегом і координатором, а громади - безпосередніми виконавцями та джерелом зворотного зв'язку. Така двостороння комунікація дозволяє узгодити національні цифрові політики з місцевими потребами, забезпечити масштабованість рішень і водночас врахувати специфіку кожного регіону.

Існує також вертикальна взаємодія через систему показників і субвенцій. Наприклад, виконання плану заходів Стратегії цифрової трансформації регіонів контролюється Міністерством цифрової трансформації спільно з Міністерством розвитку громад та територій. Області щоквартально звітують про прогрес (кількість підключених громад до інтернету, запущених послуг, навчено населення і т.д.).

Вже кілька років на конкурсній основі надаються кошти на створення нових ЦНАП чи точок Wi-Fi в селах - розподіл цих субвенцій залежить від якості заявок від громад та їх готовності співфінансувати проєкти. Зворотньою стороною такої взаємодії є відповідальність громад перед державою за дотримання єдиних стандартів. Так, ЦНАПи мають використовувати типове програмне забезпечення для електронної черги та документообігу сумісне з національними системами. Місцеві сайти і портали повинні відповідати вимогам кіберзахисту і доступності. Держава встановлює ці стандарти, а громади впроваджують. Це подібно до вертикалі цифрового управління, яка забезпечує однаковий мінімальний рівень послуг по всій країні.

Якщо громади зіштовхуються з фінансовими чи кадровими труднощами у виконанні вимог, їм надається допомога - субвенції, методична підтримка, навчання. У підсумку, така взаємодія формує мережеву модель управління, коли громади автономні у виборі шляхів розвитку, але інтегровані у загальноукраїнську цифрову інфраструктуру.

Враховуючи проаналізовані виклики і досягнення, можна окреслити конкретні шляхи удосконалення розвитку електронного урядування в

контексті забезпечення інформаційної безпеки на регіональному рівні (рис.3.2). Охарактеризуємо кожний з напрямів детально.

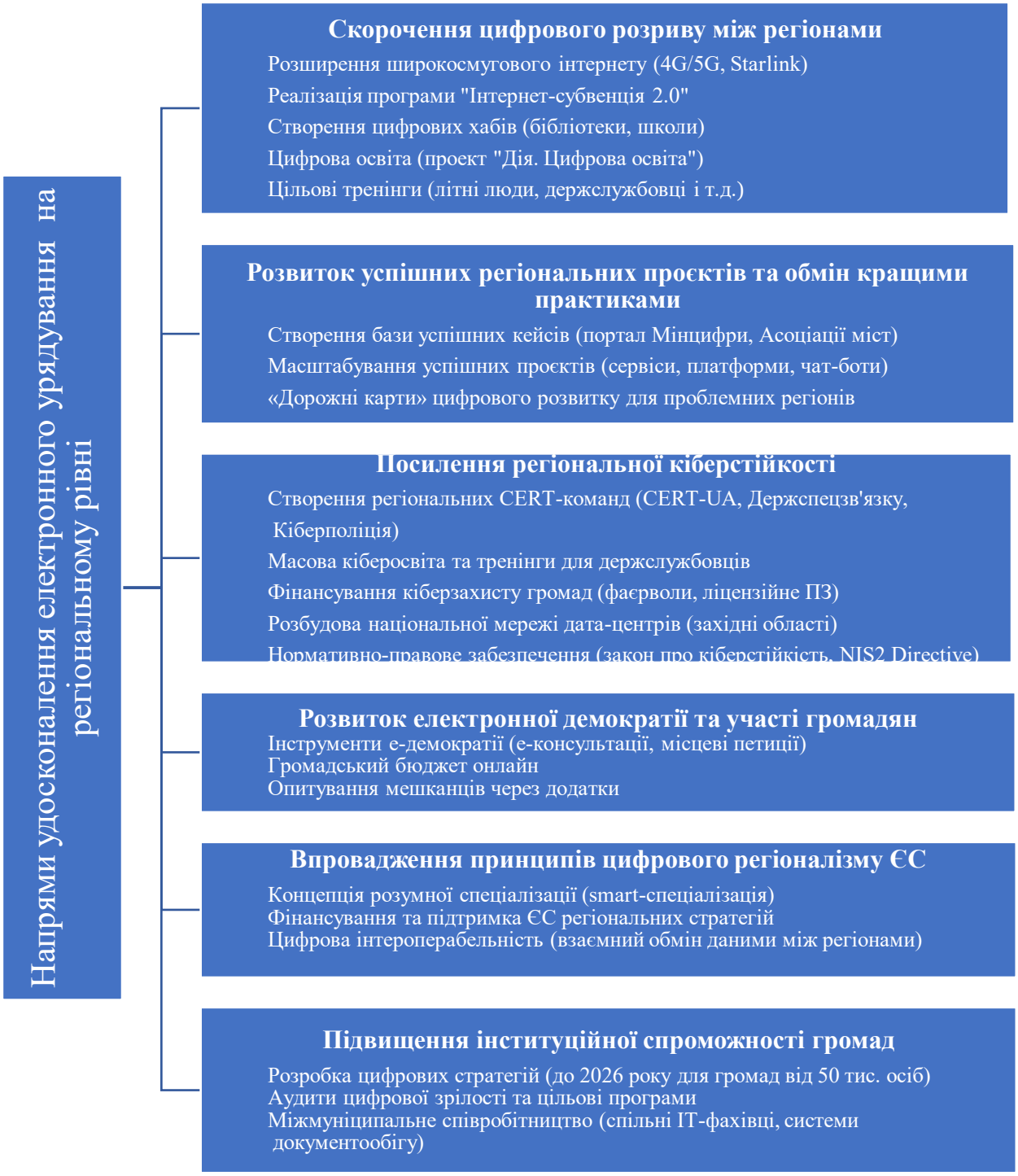


Рисунок 3.2. Напрями удосконалення електронного урядування на регіональному рівні в контексті інформаційної безпеки

Джерело: розроблено автором

Скорочення цифрового розриву між регіонами. Необхідно продовжувати ініціативи з цифрової інклюзії. Розширення широкосмугового інтернету в села (через підтримку провайдерів, розвиток 4G/5G, супутникового інтернету Starlink для важкодоступних точок), субсидування вартості інтернету для малозабезпечених верств, відкриття нових цифрових хабів у бібліотеках, школах, поштових відділеннях.

Важливим кроком стане реалізація нещодавно ухваленої державної програми «Інтернет-субвенція 2.0», що передбачає співфінансування проведення оптоволокна в кожне село з населенням понад 100 осіб до 2026 року. Навчання цифровим навичкам, масштабування проєкту «Дія. Цифрова освіта» з особливим фокусом на відстаючі регіони, курси для літніх людей, людей з інвалідністю, сільського населення. Очікуваний результат - вирівнювання базових показників, щоб у кожній області інтернет-користувачів було 80%+, а електронними послугами користувалися не менше 50% мешканців.

Розвиток успішних регіональних проєктів та обмін кращими практиками. Варто створити базу даних успішних кейсів цифровізації регіонів - своєрідний каталог проектів, впроваджених різними громадами. Така база, можливо у форматі порталу Міністерства цифрової трансформації або Асоціації міст, дозволить швидко тиражувати успішні рішення. Якщо якась область розробила зручний сервіс, уряд країни може підтримати його масштабування на інші регіони, виділивши гранти або методичну допомогу. Водночас, важливо адресно працювати з проблемними регіонами, а саме складати для них «дорожні карти» цифрового розвитку, враховуючи специфіку, для прифронтових - акцент на відновлення інфраструктури, для депресивних - на залучення інвестицій у ІТ-сектор, створення технопарків.

Посилення регіональної кіберстійкості. За цим напрямом першочерговим завданням є створення розгалуженої системи кібербезпеки від центру до громад. Пропонується у кожній області сформувати постійно діючі команди реагування на комп’ютерні надзвичайні події під егідою

Держспецзв’язку або Кіберполіції. Вони співпрацюватимуть з центральним CERT-UA, але фокусуватимуться на допомозі місцевим органам, моніторинг регіонального сегменту, аудит мереж міських рад, оперативний виїзд на інцидент у будь-яку громаду області. Такі команди вже почали формувати, але їх слід законодавчо закріпити і профінансувати. Масова кіберосвіта державних службовців може бути забезпечена через розробку курсу з основ кібергігієни обов’язкового для всіх працівників, проводити регулярні навчання і навіть імітаційні «white hat» атаки для перевірки захищеності. Передбачити в держбюджеті субвенції на засоби кіберзахисту для громад. Особливо це важливо для невеликих громад, яким самотужки не осилити дорогі рішення. Ще один напрям - розбудувати національну мережу дата-центрів для потреб регіонів, аби всі критичні дані місцевих громад зберігались у надійному резерві, можливо, на базі державно-міжнародного партнерства побудувати кілька сучасних сховищ у західних областя. Все це має доповнюватися оновленням нормативної бази, ухваленням законів про критичну інформаційну інфраструктуру і кіберстійкість громад, розробка стандартів безпеки для місцевих ІТ-систем на основі стандартів НБУ чи європейських NIS2 Directive.

Підвищення інституційної спроможності. Кожна громада повинна мати цифрову стратегію - чіткий план, інтегрований у загальну стратегію розвитку території. Уряд країни може зобов’язати всі громади з населенням більше 50 тис. осіб розробити і затвердити такі стратегії до 2027 року з урахуванням принципів smart-спеціалізації, тобто фокусуванні на власні сильні сторони. В рамках цих стратегій - провести аудити цифрової зрілості місцевих органів, щоб ідентифікувати слабкі місця. За результатами аудитів можна ініціювати цільові програми. Ще одиним інструментом може стати міжмуніципальне співробітництво, коли кілька малих громад можуть спільно утримувати ІТ-фахівця чи експлуатувати спільну систему електронного документообігу з метою оптимізації фінансових витрат.

Впровадження принципів цифрового регіоналізму ЄС. Україна прагне інтеграції до ЄС, тому важливо адаптувати європейські підходи до регіональної цифрової політики, зокрема, це концепція розумної спеціалізації регіонів. Її суть у тому, щоб кожен регіон ідентифікував кілька нішевих напрямів з високим інноваційним потенціалом і концентрував зусилля на їх цифровому розвитк. ЄС підтримує розробку регіональних стратегій і надає фінансування під ці цілі. Інший європейський принцип цифрової інтероперабельності полягає в забезпечення взаємного визнання та обміну даними між системами різних регіонів і країн.

Розвиток електронної демократії та участі громадян. Електронне урядування на регіональному рівні - це не лише про послуги, а й про нові способи взаємодії влади з людьми. Тому важливо на місцях впроваджувати інструменти електронної демократії, а саме електронні консультації, місцеві петиції, громадський бюджет онлайн, опитування мешканців через додатки. Такі міста, як Чернігів, Вінниця, Львів уже активно впроваджують дані інструменти. За умови зручних цифрових платформ мешканці активніше залучаються до вирішення питань громади, а це призводить до зростання довіри та забезпечує транспарентність місцевої влади.

Удосконалення регіональної політики в контексті розвитку електронного урядування та забезпечення інформаційної безпеки має здійснюватися на засадах системності, із належним урахуванням просторової диференціації територій та відповідності загальнонаціональним стратегічним пріоритетам. Сформульовані напрями розвитку від розширення цифрової інклюзії до зміцнення інституційної спроможності суб’єктів публічного управління та активізації участі громадян утворюють концептуальну основу формування цілісної та стійкої архітектури електронного урядування на регіональному рівні.

Водночас результативність зазначених трансформацій у значній мірі зумовлюється якістю чинного нормативно-правового регулювання, яке має враховувати як актуальні ризики та виклики у сфері інформаційної безпеки,

так і необхідність правової адаптації до законодавчого простору Європейського Союзу. Це вимагає розроблення практично орієнтованих рекомендацій щодо вдосконалення чинного нормативно-правового регулювання з урахуванням принципів кіберстійкості, відкритості, громадської участі та євроінтеграційних процесів.

3.3. Практичні рекомендації щодо вдосконалення нормативно-правового забезпечення інформаційної безпеки в електронному урядуванні

Враховуючи зростання цифрових загроз та виклики, пов'язані з необхідністю гармонізації національного законодавства з європейськими стандартами у сфері інформаційної безпеки, важливим є формулювання практичних рекомендацій щодо вдосконалення нормативно-правового забезпечення електронного урядування. Ми розробили конкретні пропозиції з акцентом на впровадження сучасних принципів інформаційної безпеки, активізацію участі громадськості та адаптацію національного законодавства до європейських норм.

Одним із ключових напрямів нормативно-правового вдосконалення у сфері інформаційної безпеки електронного урядування є створення умов для комплексного впровадження принципу «zero trust» («нульова довіра») в інформаційні системи державних органів та органів місцевого самоврядування. Даний підхід, що розглядається в сучасній науковій і прикладній літературі [48] як один із найефективніших у контексті побудови кіберстійких цифрових архітектур, передбачає цілковите усунення апріорної довіри до будь-яких користувачів або пристроїв, незалежно від їхнього місцезнаходження в межах або поза межами периметра інформаційної системи.

В умовах стрімкої цифровізації публічних сервісів та зростання загроз як зовнішнього, так і внутрішнього характеру, зокрема, у вигляді соціотехнічних атак, компрометації ідентифікаційних даних, вразливостей у

міжвідомчих каналах обміну інформацією, реалізація принципу «нульової довіри» дозволяє суттєво знизити ризики несанкціонованого доступу, витоків конфіденційної інформації та порушень цілісності цифрових державних систем.

З правової точки зору впровадження моделі Zero Trust Architecture [48] потребує чіткого нормативного закріплення її як одного з базових принципів організації інформаційної безпеки в публічному секторі. Зокрема, першочерговим кроком до реалізації зазначеної ініціативи має стати розроблення і затвердження нормативно-правового акту центрального рівня, постанови Кабінету Міністрів України, якою визначатиметься обов'язковість впровадження принципу «zero trust» у структурі інформаційних систем усіх органів виконавчої влади, органів місцевого самоврядування та суб'єктів, що здійснюють обробку критично важливої або чутливої інформації (персональні дані громадян, медичні реєстри, платіжні системи, дані оборонного характеру тощо).

Окрему увагу слід приділити необхідності внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України» [25], в якому доцільно передбачити визначення принципу «нульової довіри» як концептуальної складової системи інформаційної безпеки. У тексті закону варто зазначити вимогу дотримання принципів багаторівневої автентифікації, найменших привілеїв, постійного моніторингу дій користувачів, сегментації доступу та верифікації ідентичності у всіх точках входу до системи.

Для забезпечення практичної реалізації принципу «нульової довіри» доцільним є формування відповідної нормативної та методологічної бази. Це передбачає розроблення державних стандартів або затвердження національних технічних регламентів, які б відповідали міжнародним стандартам, зокрема ISO/IEC 27001, щодо побудови систем управління інформаційною безпекою та рекомендаціям NIST SP 800-207, щодо архітектури нульової довіри. Доцільно створити централізований реєстр таких документів на платформі Національного координаційного центру

кібербезпеки при РНБО або Міністерства цифрової трансформації України, який стане базою знань для фахівців державного сектору.

Крім того, важливим елементом реалізації зазначеного є впровадження обов'язкових аудитів інформаційної безпеки державних органів, у тому числі з перевіркою відповідності інформаційних систем принципу «zero trust». Такий аудит може здійснюватися на основі єдиної методики оцінювання рівня кіберстійкості за участю незалежних експертів або через створення спеціалізованих внутрішніх аудитних підрозділів у державних органах. Результати перевірок мають бути основою стратегічного планування заходів із посилення кібербезпеки та стати підґрунтям для перерозподілу бюджетних коштів, спрямованих на цифрову трансформацію.

Нормативне закріплення принципу «нульової довіри» як обов'язкового стандарту в електронному урядуванні України, у поєднанні з його технічною імплементацією та відповідним моніторингом, створить системну основу для формування надійного, адаптивного та стійкого цифрового середовища, що відповідає сучасним вимогам інформаційної безпеки та євроінтеграційним прагненням України

Залучення громадськості до механізмів контролю за інформаційною безпекою не лише сприяє формуванню довіри до цифрової держави, а й забезпечує більш ефективне функціонування системи електронного урядування шляхом своєчасного виявлення вразливостей, запобігання зловживанням і сприяння дотриманню етичних норм використання цифрових технологій. На законодавчому рівні доцільно започаткувати чітко врегульовану процедуру громадського аудиту інформаційної безпеки в державному секторі. Для цього необхідно внести доповнення до Закону України «Про основні засади забезпечення кібербезпеки України» [25]. Зокрема, доцільно включити нову статтю, яка б визначала правовий статус і порядок ініціювання громадського аудиту, механізм взаємодії громадських об'єднань та експертних організацій з уповноваженими суб'єктами у сфері кібербезпеки, а також вимоги до звітності державних органів щодо результатів

таких перевірок. Уточнення також потребує стаття 7 цього ж Закону, яка визначає принципи державної політики у сфері кібербезпеки, пропонується додати принцип публічності та громадської участі у формуванні й реалізації кіберполітик.

У Законах України «Про електронну ідентифікацію та електронні довірчі послуги» [17] та «Про електронні документи та електронний документообіг» [16] доцільно передбачити положення про обов'язковість попередніх консультацій з громадськістю перед запровадженням нових державних електронних послуг або функціоналу. Запровадження відповідної процедури має забезпечити врахування громадської думки на етапі планування та розробки електронних сервісів. Рекомендовано включити у законодавчий текст окремий підрозділ, який би визначав мінімальні вимоги до консультацій, тобто їх тривалість, формат (онлайн-опитування, публічні обговорення), способи оприлюднення проектів рішень та обов'язковість врахування зауважень.

Особливої уваги потребує імплементація положень щодо використання відкритих даних про стан інформаційної безпеки в державному секторі. Закон України «Про доступ до публічної інформації» [15] повинен бути доповнений положенням, що зобов'язує органи державної влади публікувати дані про кіберінциденти, статистику звернень користувачів щодо проблем захищеності, інформацію про аудит безпеки цифрових сервісів, а також звіти про впровадження заходів реагування на виявлені загрози. Публікація цієї інформації має відбуватися у форматі відкритих даних на Єдиному державному вебпорталі відкритих даних (data.gov.ua), з урахуванням вимог захисту державної та конфіденційної інформації.

Окрім цього, у Закон України «Про звернення громадян» [19] варто інтегрувати окремий розділ щодо специфіки розгляду звернень громадян, пов'язаних із питаннями захищеності електронних державних послуг. Зокрема, має бути передбачено скорочений термін розгляду звернень, що стосуються безпеки персональних даних або інцидентів порушення

конфіденційності, а також зобов’язання органів виконавчої влади забезпечити публічну відповідь із описом вжитих заходів.

З метою підвищення ролі громадськості в ухваленні стратегічних рішень у сфері інформаційної безпеки, пропонується розробити та затвердити Положення про громадські ради з питань цифрової трансформації та інформаційної безпеки. Ці ради можуть функціонувати при центральних, Міністерстві цифрової трансформації, та місцевих органах виконавчої влади, надаючи рекомендації щодо нормативного регулювання, контролю за впровадженням заходів кібербезпеки, забезпечення прозорості в роботі цифрових сервісів. На рівні підзаконних актів Кабінету Міністрів України можливо визначити стандартний регламент діяльності таких рад, порядок їх формування та принципи добору представників громадянського суспільства.

Важливим інструментом підвищення громадської довіри до державних цифрових платформ може стати впровадження системи громадського моніторингу, базованої на онлайн-платформах. З огляду на європейські практики, наприклад, «e-Participation Toolkit» Єврокомісії, в Україні доцільно запровадити уніфікований онлайн-інструмент, де користувачі можуть повідомляти про проблеми з інформаційною безпекою сервісів, оцінювати якість послуг та надавати зворотний зв’язок.

Нарешті, необхідно закріпити принцип публічної звітності про ефективність заходів з інформаційної безпеки, який має стати частиною щорічних звітів усіх центральних органів виконавчої влади, які надають електронні послуги. Закон України «Про Кабінет Міністрів України» [86] може бути доповнений положенням, що передбачає подання Міністерством цифрової трансформації щорічного звіту про стан інформаційної безпеки державних інформаційних ресурсів та рівень участі громадськості в їх захисті.

Реалізація вищезазначених пропозицій дозволить сформувати прозору, публічну та підзвітну модель цифрового врядування, де громадяни виступають не лише пасивними користувачами сервісів, а й активними суб’єктами впливу на політику інформаційної безпеки. Такий підхід

відповідає принципам належного врядування, викладеним у документах Ради Європи, а також відображає імперативи демократизації державного управління в умовах цифрової епохи.

Залучення громадськості до сфери забезпечення інформаційної безпеки слід розглядати не як формальний інструмент підзвітності органів влади, а як один із базових принципів стійкої цифрової держави, що відповідає європейським стандартам належного урядування. Зокрема, у концепціях цифрового громадянства, розроблених під егідою Ради Європи, наголошується на пріоритетності прозорості, етичності цифрової політики та зобов'язанні держави забезпечити інклюзивну участь у всіх етапах розробки й реалізації цифрових рішень.

У сучасній нормативно-правовій базі України відсутня цілісна система правових інструментів, яка б регламентувала залучення громадянського суспільства до нагляду за реалізацією політики інформаційної безпеки у сфері електронного урядування. У зв'язку з цим доцільно ініціювати низку змін до чинного законодавства, спрямованих на запровадження нових процедур і уточнення існуючих норм.

Передусім, необхідно передбачити в законодавстві України можливість громадського аудиту інформаційної безпеки, який має здійснюватися акредитованими громадськими або експертними організаціями на добровільних засадах у межах чіткого регламенту. Цей механізм слід законодавчо закріпити шляхом внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України» [25]. Рекомендовано доповнити цей закон окремим розділом або статтею, в якій визначити правові умови ініціювання громадського аудиту, критерії добору акредитованих суб'єктів, процедури інформування державних органів, обов'язок надання публічної відповіді та обов'язковість розгляду висновків таких перевірок.

З метою створення постійно діючих платформ громадської участі, необхідно розробити нормативно-правовий акт у формі постанови Кабінету Міністрів України, що регламентує створення та функціонування громадських

рад з питань цифрового врядування та інформаційної безпеки при центральних та регіональних органах виконавчої влади. У цьому документі варто чітко визначити їхні повноваження щодо здійснення консультативного нагляду за дотриманням принципів прозорості, належного захисту персональних даних, обробки відкритих даних, та відповідності державних цифрових платформ базовим принципам інформаційної безпеки. Особливої уваги потребує унормування права таких рад отримувати доступ до релевантної публічної інформації та мати право брати участь у розробці нормативно-правових актів у сфері електронного урядування.

Окрему увагу слід приділити використанню відкритих даних у сфері інформаційної безпеки як інструменту громадського контролю. Пропонується доповнити Закон України «Про доступ до публічної інформації» [15] та Закон України «Про Національну інфраструктуру геопросторових даних» [22] положеннями, які зобов'язуватимуть органи влади оприлюднювати у форматі відкритих даних інформацію про інциденти кібербезпеки, вжиті заходи реагування, регулярні результати технічних аудитів безпеки цифрових систем, а також щоквартальні звіти про індикатори прозорості державних електронних послуг. Важливо забезпечити технічну та юридичну можливість незалежного аналізу цих даних недержавними аналітичними центрами та експертними спільнотами.

Крім того, перспективним напрямом є впровадження практики попереднього громадського обговорення нових електронних державних сервісів. Для цього в Законі України «Про електронні довірчі послуги» та Законі України «Про електронні документи та електронний документообіг» доцільно передбачити норму, яка встановлюватиме обов'язковість електронних консультацій із громадськістю при запровадженні функціонально нових державних цифрових інструментів. Це дозволить враховувати потреби користувачів, підвищувати їхню довіру до сервісів, а також виявляти можливі ризики на етапі проєктування систем.

Для забезпечення правових гарантій реалізації зазначених підходів пропонується розробити і прийняти окремий нормативно-правовий акт «Концепцію участі громадянського суспільства у забезпеченні інформаційної безпеки держави», яка б закладала засади довгострокової взаємодії держави з громадськими структурами у сфері цифрового врядування та кіберзахисту. У межах цієї Концепції доцільно також передбачити механізми фінансування та навчання представників громадськості для участі у відповідних процесах, що сприятиме зростанню цифрової грамотності та відповідальності громадянського суспільства. Всі зміни нормативно-правової бази які запропоновані в контексті нашого дослідження представлені в таблиці 3.1.

Загалом, правове врегулювання участі громадськості у сфері інформаційної безпеки має спиратися на засади прозорості, відкритості, партисипативності й кооперації, які лежать в основі європейської моделі цифрової демократії.

Таблиця 3.1. Пропозиції щодо внесення змін в нормативно-правове забезпечення інформаційної безпеки електронного урядування

Закон України	Запропоновані зміни	Мета змін
Про основні засади забезпечення кібербезпеки України	Закріпити принцип «нульової довіри» як обов'язковий стандарт, визначити вимоги багаторівневої автентифікації, моніторингу, сегментації доступу, та механізми громадського аудиту кібербезпеки	Зниження ризиків несанкціонованого доступу та витоку інформації, формування кіберстійкої екосистеми державних інформаційних ресурсів
Про електронну ідентифікацію та електронні довірчі послуги	Запровадження обов'язкових попередніх консультацій з громадськістю перед запровадженням нових електронних послуг	Забезпечення прозорості розробки цифрових сервісів, підвищення довіри громадськості
Про електронні документи та електронний документообіг		
Про доступ до публічної інформації	Обов'язковість публікації даних про кіберінциденти, аудити безпеки у форматі відкритих даних	Посилення громадського контролю за безпекою цифрових послуг, підвищення прозорості дій влади
Про звернення громадян	Інтегрувати окремий розділ щодо специфіки розгляду звернень громадян з питань інформаційної безпеки з скороченими термінами реагування	Оперативне реагування на інциденти інформаційної безпеки, підвищення рівня захисту персональних даних
Про Кабінет Міністрів України	Подання щорічного звіту про стан інформаційної безпеки та участь громадськості в її забезпеченні	Системне інформування громадськості про стан кібербезпеки, прозорість та підзвітність органів влади
Про Національну інфраструктуру геопросторових даних	Публікація регулярних звітів про результати аудитів безпеки цифрових систем, кіберінциденти, прозорість послуг	Забезпечення прозорості та громадського контролю за інформаційною безпекою цифрових ресурсів

Джерело: розроблено автором

Висновки до розділу 3

У третьому розділі дисертаційної роботи сформульовано стратегічні напрями та нормативно-правові засади розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки. Основні результати проведеного дослідження дають підстави для висновків.

1. Сформульовано систему стратегічних напрямів розвитку електронного урядування з урахуванням чинників інформаційної безпеки на основі поетапного підходу - короткострокової, середньострокової і довгострокової перспектив. Визначено, що ключовими є впровадження принципу «безпеки за замовчуванням», оновлення законодавства, інституційна координація, цифрова просвіта населення, архітектура «нульової довіри», євроінтеграція в сфері цифрових стандартів, розвиток електронної демократії та механізмів довіри.

2. Обґрунтовано напрями розвитку електронного урядування на регіональному рівні, які включають подолання цифрової нерівності між областями, запровадження регіональних цифрових стратегій і центрів кібербезпеки, посилення інституційної спроможності громад, а також формування умов для співробітництва між громадами. Зроблено акцент на необхідності адаптації кращих європейських практик зокрема, принципів розумної спеціалізації регіонів, цифрової інтероперабельності та відкритості даних.

3. Запропоновано нормативно-правові умови впровадження принципу «нульової довіри» у державному управлінні, що передбачають внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України», ухвалення урядової постанови про обов’язковість «нульової довіри» для захищених ІТ-систем, а також розробку національних стандартів і методичних рекомендацій на основі міжнародних вимог (ISO 27001, NIST SP 800-207).

4. Обґрунтовано необхідність нормативного закріплення механізмів громадського контролю у сфері інформаційної безпеки електронного

урядування, включаючи правове регулювання громадського аудиту, створення консультативних рад при органах влади, розширення доступу до відкритих даних про стан кібербезпеки, а також обов’язкове проведення публічних консультацій з громадянами перед впровадженням нових електронних сервісів. Підкреслено, що такі механізми є критично важливими для формування довіри до цифрових інструментів держави.

5. Сформульовано конкретні рекомендації щодо адаптації українського законодавства до цифрового acquis Європейського Союзу. Визначено пріоритети нормативного забезпечення у сфері захисту персональних даних, регулювання штучного інтелекту, використання довірчих послуг, забезпечення кіберстійкості критичної цифрової інфраструктури та міжрегіональної інтероперабельності.

Основні положення розділу дисертаційної роботивідображені в працях автора [34, 35, 121]

ВИСНОВКИ

У дисертаційній роботі сформульовано та обґрунтовано нові теоретичні та прикладні підходи, які в сукупності забезпечують вирішення актуального наукового завдання у сфері публічного управління. Зокрема, йдеться про розробку концептуальних основ і методологічних засад розвитку електронного урядування України в умовах забезпечення інформаційної безпеки, а також підготовку практичних рекомендацій щодо їх ефективної реалізації в сучасних умовах.

1. Розкрито сутність електронного урядування як сучасної форми цифрового публічного управління, з'ясовано його функціональні характеристики, базові принципи та його місце в системі державного управління в умовах цифрової трансформації. Встановлено, що електронне урядування є не лише інструментом автоматизації адміністративних функцій, а системним чинником оновлення моделей взаємодії між державою, громадянами та бізнесом. Доведено, що впровадження цифрових технологій має супроводжуватись переосмисленням управлінських процесів на основі принципів цифровізації даних та сервісної орієнтації.

2. Сформовано концептуальне бачення інформаційної безпеки у системі електронного урядування, визначено її роль як інтегральної складової цифрового публічного управління. Узагальнено основні принципи превентивності, нульової довіри, багаторівневого захисту, відповідальності суб'єктів, структурно виокремлено ключові елементи технічної безпеки, кібергігієни, нормативного забезпечення, цифрової грамотності персоналу та встановлено функціональний взаємозв'язок інформаційної безпеки з поняттям цифрової довіри. Аргументовано, що забезпечення інформаційної безпеки має бути не реактивною, а проактивною функцією електронного урядування.

3. Проаналізовано міжнародний досвід забезпечення інформаційної безпеки в електронному урядуванні, зокрема практики ЄС, США, Естонії, Сінгапуру, Південної Кореї. Виявлено типові моделі цифрової безпеки

публічного сектору, а саме архітектура «zero trust», розвинуті системи цифрової ідентифікації, незалежні агентства з кіберзахисту, обов'язкові програми цифрової освіти для державних службовців. Визначено, що успішні системи електронного уряду базуються на законодавчо визначених вимогах кібербезпеки, інституційному лідерстві та високому рівні залучення громадськості до процесів контролю за прозорістю цифрових послуг.

4. Оцінено сучасний стан системи електронного урядування в Україні, встановлено такі ключові досягнення, як масштабна цифровізація державних послуг, поява платформи «Дія», збільшення охоплення інтернет-користувачів, а також ідентифіковано низку проблем в частині нерівномірного цифрового розвитку між регіонами, обмеженні інтегрованості реєстрів, незадовільного рівня міжвідомчої координації, неготовності окремих верств населення до використання електронних сервісів.

5. Проаналізовано нормативно-правове забезпечення функціонування електронного урядування в Україні, виявлено суттєві прогалини у законодавстві щодо захисту персональних даних, застосування хмарних технологій, штучного інтелекту, а також імплементації стандартів ЄС (GDPR, NIS2, AI Act). Підкреслено потребу синхронізації українських актів з європейським правовим простором та необхідність систематизації цифрового законодавства через кодифікацію норм, що регулюють електронне урядування.

6. Систематизовано загрози та ризики інформаційної безпеки в електронному урядуванні, що мають як внутрішню (низька кваліфікація персоналу, технічні вразливості, неналежне адміністрування систем), так і зовнішню (кібератаки з боку агресивних держав, шпигунство, злом реєстрів) природу походження. Аргументовано, що з початком широкомасштабної війни зросла потреба у кіберстійкості не лише на національному, а й на регіональному рівні.

7. Обґрунтовано стратегічні напрями розвитку системи електронного урядування в Україні, структуровані за трьома часовими горизонтами –

коротко-, середньо- та довгостроковим. Визначено основні напрями, серед яких інтеграція інформаційної безпеки в стратегії цифровізації державних сервісів, модернізація нормативної бази, розвиток електронної ідентичності, регіональна кіберстійкість, імплементація «нульової довіри», гармонізація із законодавством ЄС та побудова системи цифрової демократії.

8. Визначено перспективи розвитку електронного урядування на регіональному рівні, де особливу увагу приділено питанням цифрової інклюзії, локальної кібербезпеки, залучення громадян до електронної участі, а також інституційної спроможності громад формувати власні цифрові стратегії. Узагальнено практики регіонів України, які можуть слугувати прикладами для впровадження національних рішень.

9. Розроблено комплекс практичних рекомендацій щодо вдосконалення нормативно-правового забезпечення інформаційної безпеки електронного урядування, зокрема щодо впровадження принципу «нульової довіри» у законодавство; створення механізмів громадського контролю за кібербезпекою; запровадження обов’язкових електронних консультацій; регламентування публічного доступу до відкритих даних про стан цифрової безпеки; адаптації українських актів до норм ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александрова М. В. Адміністративно-правове забезпечення інформаційної безпеки у сфері електронного урядування : дис. … доктора філософії за спец. 081 Право. Київ : Міжрегіональна Академія управління персоналом, 2024. 160 с.

2. Бакуменко В. Д. Електронне урядування як складова сучасного державного управління // Електронне урядування. 2010. № 1. С. 5-15. Режим доступу: https://ktpu.kpi.ua/wp-content/uploads/2016/02/ZHurnal_Elektronne-uryaduvannya_1_2010.pdf.

3. Бермас, А. Міжнародний досвід діджиталізації діяльності органів державної влади. Аспекти публічного управління, 12(4), 2024. С.13-18. https://doi.org/10.15421/152443

4. Велігура А. В. Дослідження шляхів розробки комплексів інформаційної безпеки / А. В. Велігура, Л. М. Дегтярьова, О. М. Степанова // Вісник Східноукраїнського національного університету імені В. Даля. 2009. № 6(136), Ч. 1. С. 154-161. Режим доступу: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf

5. Вітчизняний і зарубіжний досвід впровадження електронного урядування [Електронний ресурс] // Кафедра теорії та практики управління // НТУУ «КПІ». - Режим доступу: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Vitchiznyanij-i-zarubizhnij-dosvid-vprovadzhennya-elektronnogo-uryaduvannya.pdf

6. Гайдученко С. О. Електронне урядування: конспект лекцій для студентів усіх форм навчання спеціальності 281 - Публічне управління та адміністрування / С. О. Гайдученко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 54 с.

7. Гнатюк С. М. Інформаційна безпека України в умовах євроінтеграції: виклики та перспективи [Електронний ресурс] / С. М. Гнатюк

// Національний інститут стратегічних досліджень. - 2015. Режим доступу: https://www.niss.gov.ua/sites/default/files/2015-02/Gnatyuk-59546.pdf

8. Головний ситуаційний центр кібербезпеки при РНБО України [Електронний ресурс]. - Режим доступу: https://cip.gov.ua/ua

9. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Н. Дереко // Інформаційна безпека людини, суспільства, держави. 2015. № 2(18). С. 16-22.

10. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки / О. Д. Довгань // Інформація і право. 2015. № 2(14).

11. Домбровська С. М. Механізми формування безпеки держави [Електронний ресурс] / С. М. Домбровська, С. Т. Полторак // Теорія та практика державного управління і місцевого самоврядування. 2015. № 1. Режим доступу: http://el-zbirn-du.at.ua

12. Дубов Д.В., Дубова С.В. Основи електронного урядування: навчальний посібник. Київ : Центр навчальної літератури, 2006. 176 с.

13. Економіка та держава: міжнародний науково-практичний журнал [Електронний ресурс]. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5514

14. Жиляєв І. Б., Семенченко А. І. Етапи розвитку електронного урядування: сутність та термінологія // Теорія та практика державного управління. 2019. № 1(64). С. 17–30.

15. Закон України «Про доступ до публічної інформації» № 2939-VI від 13.01.2011 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text

16. Закон України «Про електронні документи та електронний документообіг» № 851-IV від 22.05.2003 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text

17. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text

18. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

19. Закон України «Про звернення громадян» від 02.10.1996 № 393/96-ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/main/393/96-%D0%B2%D1%80#Text.

20. Закон України «Про інформацію» № 2657-XII від 02.10.1992 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

21. Закон України «Про Кабінет Міністрів України» від 27.02.2014 № 794-VII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/794-18#Text

22. Закон України «Про національну інфраструктуру геопросторових даних» від 13.04.2020 № 554-IX [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/554-20#Text

23. Закон України «Про Національну програму інформатизації» № 74/98-ВР від 04.02.1998 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text

24. Закон України «Про основи національної безпеки України» № 964-IV від 19.06.2003 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/964-15#Text

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

26. Закон України «Про хмарні послуги» № 2075-IX від 17.02.2022 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2075-20#Text

27. Знання.орг. Електронне урядування: міжнародний досвід [Електронний ресурс] // Znannya.org: освітній портал. - Режим доступу: http://www.znannya.org/?view=e-government-experience

28. Ільницький, М. П. Адміністративно-правові засади електронного урядування у сфері публічного управління в Україні [Електронний ресурс] / М. П. Ільницький // Науковий вісник Ужгородського національного університету. Серія «Право». - 2020. - Вип. 60. - С. 116-121. - Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/32975/1/АДМІНІСТРАТИВНО-ПРАВОВІ%203АСАДИ%20ЕЛЕКТРОННОГО%20УРЯДУВАННЯ.pdf

29. Індекс цифрової трансформації регіонів України - 2023 [Електронний ресурс] / Міністерство цифрової трансформації України. - Київ, 2023. - Режим доступу: https://thedigital.gov.ua/storage/uploads/files/page/community/reports/Індекс-цифрової-трансформації-регіонів-України-2023.pdf.

30. Інституційні засади управління інформаційною безпекою держави [Електронний ресурс]. Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/21451/1/333-335.pdf

31. Інформаційна безпека (соціально-правові аспекти) : підручник / В. Остроухов, В. Петрик, М. Присяжнюк та ін. ; за ред. Є. Д. Скулиша. Київ: КНТ, 2010. 776 с.

32. Інформаційна безпека: сучасні виклики та загрози [Електронний ресурс]. Режим доступу: https://er.nau.edu.ua/server/api/core/bitstreams/53d39063-8c63-4ace-92f7-edb1771d7468/content

33. Інформаційна політика: навчальний посібник / Г. Почепцов, С. Чукут. Київ : Знання, 2008. 663 с.

34. Кутова М. А. Ідентифікація стратегічних напрямів розвитку системи електронного урядування в контексті інформаційної безпеки. Вісник Хмельницького національного університету. Серія: Економічні науки, 2025, №2. - с.60-63. https://doi.org/10.31891/2307-5740-2025-340-8

35. Кутова М. А. Модель стратегічного планування розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки.

Вісник Хмельницького національного університету. Серія: Економічні науки, 2025, №3. - с.12-16. https://doi.org/10.31891/2307-5740-2025-342-3(1)-1

36. Кутова М.А. Основні загрози та ризики інформаційної безпеки в електронному урядуванні України. International scientific-practical conference “Economics, accounting, finance and management: strategic priorities for development in the context of globalization”: conference proceedings (Tampere, Finland, March 21, 2025). Tampere, Finland: Scholarly Publisher ICSSH, 2025. 37 pages. (c.30-34).

37. Кутова М. А. Теоретичні аспекти становлення електронного урядування в Україні. Юність науки - 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). - Чернігів: НУ «Чернігівська політехніка», 2023. - 770 с. (с. 213)

38. Концептуальні засади розвитку електронного урядування в Україні : навчальний посібник / за ред. А. І. Семенченка. Київ, 2009. 82 с

39. Концепції розвитку електронного урядування в Україні. Схвалено розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р [Електронний ресурс] // Офіційний портал Верховної Ради України. - Режим доступу: https://zakon.rada.gov.ua/laws/show/649-2017-p#Text

40. Концепція розвитку штучного інтелекту в Україні [Електронний ресурс] : схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. - Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

41. Котляр А. М. Міжнародний досвід впровадження електронного урядування та можливості для України [Електронний ресурс] / А. М. Котляр // Вісник економіки транспорту і промисловості. - 2024. - № 58. - С. 65-72. - Режим доступу: http://vestnik-econom.mgu.od.ua/journal/2024/58-2024/11.pdf

42. Кравченко О. О. Сутність та значення електронного урядування в умовах інформаційного суспільства [Електронний ресурс] / О. О. Кравченко //

Вісник міжнародного університету. Серія: Економіка і право. - 2013. - Вип. 9. - С. 48-53. Режим доступу: https://vmv.kymu.edu.ua/series/vipusk9/11.pdf

43. Лупенко, Ю. О., Струк, О. С. Цифровізація економіки України: сучасні тенденції та перспективи розвитку [Електронний ресурс] // Актуальні аспекти розвитку економіки. - 2023. - № 20. - С. 50-59. - Режим доступу: https://aab-economics.kmf.uz.ua/aabe/article/view/194

44. Маращук А. І. Інформаційні ресурси держави: зміст та проблеми захисту [Електронний ресурс]/А.І. Маращук. Режим доступу: http://www.ndcpi.org.ua

45. Маргасова В., Руденко О., Попело О., Косач І., Сакун О., Клименко Т. Механізми державного управління розвитком цифрових технологій у системі національної безпеки [Електронний ресурс] // Revista de la Universidad del Zulia. - 2023. - Т. 15, № 42. - С. 389-406. - Режим доступу: https://doi.org/10.46925/rdluz.42.22.

46. Мельниченко В. І. Інформаційна безпека в системі електронного урядування: основні загрози та напрями їх подолання [Електронний ресурс] / В. І. Мельниченко // Державне управління: удосконалення та розвиток. - 2012. - № 4. - Режим доступу: http://pa.stateandregions.zp.ua/archive/4_2012/5.pdf

47. Міністерство цифрової тарнсформаціїї України (офіційний сайт) https://thedigital.gov.ua/

48. Національний інститут стандартів і технологій (NIST). Національний центр передового досвіду в галузі кібербезпеки (NCCoE). Проєкт «Zero Trust Architecture». - Режим доступу: https://web.archive.org/web/20210422024921/https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

49. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія / А. Ю. Нашинець-Наумова. Київ : Видавничий дім «Гельветика», 2017. 168 с. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/06.

50. Євсюкова О.В., Кузменкова К.С. Формування інституційно-правових засад протидії дезінформації в Україні. Наукові перспективи. 2024. № 10(52). С.119-128. DOI: https://doi.org/10.52058/2708-7530-2024-10(52)-119-128

51. Лашук О.С., Лілікович П.В., Сенченко І.В. Шляхи удосконалення державних механізмів у сфері національної безпеки. Публічне управління та адміністрування в Україні. 2024. №42. С.147-150.

52. Обушна Н., Теплов С. Цифровізація управління HR-процесами на державній службі Наукові перспективи. 2021. Випуск 3 (9). С. 157-171. URL: http://perspectives.pp.ua/index.php/np/article/view/183

53. Олійченко, І. М. Впровадження інструментів електронного урядування в системі державної влади / І. М. Олійченко, Ю. Д. Юрченко // Вісник Чернігівського державного технологічного університету. Серія: Економічні науки. - 2013. - № 2 (66). - С. 435-442.

54. Олійченко, І. М. Шляхи формування та удосконалення електронного урядування в системі органів державної влади / І. М. Олійченко, М. Ю. Дітковська // Вісник Чернігівського державного технологічного університету. Серія: Економічні науки. - 2013. - № 4 (70). - С. 475-482.

55. Організація Об'єднаних Націй в Україні. Перехідна рамкова програма ООН для України на 2022-2023 роки [Електронний ресурс]/ Організація Об'єднаних Націй в Україні. - Київ, 2022. - 32 с. - Режим доступу: https://ukraine.un.org/sites/default/files/2023-05/Ukr_UN%20Transitional%20Framework_19.10.pdf

56. Офіційний портал «Дія». Режим доступу: https://diia.gov.ua.

57. Перелік категорій кіберінцидентів [Електронний ресурс] // CERT-UA. - Режим доступу: https://cert.gov.ua/recommendation/16904

58. Петров В. Стан захищеності інформаційних ресурсів України та шляхи її вдосконалення // Актуальні проблеми міжнародної безпеки: український вимір. - К.: ВД “Стилос”, 2010. - С. 577.

59. План заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України : затв. розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163-р [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text.

60. Положення про Міністерство цифрової трансформації [Електронний ресурс] : постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856. - Режим доступу: https://zakon.rada.gov.ua/laws/show/856-2019-п#n12

61. Програма розвитку ООН в Україні. Аналітичний звіт «Думки і погляди населення України щодо державних електронних послуг у 2023 році» [Електронний ресурс]. - Київ: ПРООН в Україні, 2023. - Режим доступу: https://www.undp.org/uk/ukraine/publications/analitychnyy-zvit-dumky-i-pohlyady-naselennya-ukrayiny-shchodo-derzhavnykh-elektronnykh-posluh-u-2023-rotsi

62. Програма розвитку ООН в Україні. Стратегічне партнерство ООН - Україна: презентація Рамкової програми партнерства на 2023-2027 роки [Електронний ресурс] / Програма розвитку ООН в Україні. - Київ, 2022. - 21 с. - Режим доступу: https://niss.gov.ua/sites/default/files/2022-01/prezentaciya-ukrainskoyu_0.pdf

63. СБУ відбила понад 9000 кібератак за два роки повномасштабної війни [Електронний ресурс] // Forbes Україна. - 2024. - 5 березня. - Режим доступу: https://forbes.ua/news/sbu-vidbila-ponad-9000-kiberatak-za-dva-roki-povnomasshtabnoi-viyni-05032024-19667

64. Стратегія кібербезпеки України : затв. Указом Президента України від 26 серпня 2021 р. № 447/2021 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

65. У 2022 році кількість кібератак на Україну зросла майже втричі: 90 хакерських груп з РФ контролюють силовики [Електронний ресурс] // Forbes Україна. - 2023. - 4 травня. - Режим доступу: https://forbes.ua/news/v-

2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454

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

67. Фонд Східна Європа. Електронне урядування для підзвітності влади та участі громадян (EGAP). Режим доступу: https://egap.in.ua/

68. Харченко Л. С. Інформаційна безпека України: глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов ; за заг. ред. д-ра юрид. наук, проф. Р. А. Калюжного. Київ : Текст, 2011. 180 с.

69. Цифрова грамотність населення України - 2023: звіт за результатами дослідження/Міністерство цифрової трансформації України, Фонд Східна Європа. - Київ, 2023. - 68 с. - Режим доступу: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf.

70. Чукут С. А., Загвойська О. В., Цимбаленко Я. Ю. Основи електронного урядування: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2022. 244 с.

71. Щорічний звіт про кіберінциденти в Україні за 2022 рік [Electronic resource] / Державний центр кіберзахисту. - 2023. - Режим доступу: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf

72. Юридична сила електронних документів [Electronic resource] // Вчасно. - Режим доступу: https://vchasno.ua/yurydychna-syla-elektronnykh-dokumentiv/

73. Ющенко Н. В. Електронне урядування в Україні: стан та перспективи розвитку [Electronic resource] / Н. В. Ющенко, М. В. Ковтун // Причорноморські економічні студії : економічн. наук.-практ. журн. - 2019. - № 38. - Режим доступу: http://bses.in.ua/journals/2019/38_1_2019/31.pdf

74. Ahmed M. M., Ahmed A. M. Citizens' Data Protection in E-government System // International Journal of Innovative Computing. 2023. 13(2). С. 1–9. DOI: 10.11113/ijic.v13n2.389

75. Bora and Information Security Buzz. AI Governance Regulation Tracker: 2025 Edition [Electronic resource] / Bora, ISBuzz News. - 2024. - 22 с. - Режим доступу: https://informationsecuritybuzz.com/wp-content/uploads/Bora-and-ISB-AI-Governance-Reg-Tracker.pdf

76. Crossing borders: Security and privacy issues of the European e-passport. /Hoepman, J.H.; Hubbers, E.; Jacobs, B.P.F. et al. s.n., 2008. (CoRR; Vol. abs/0801.3930).

77. Cybersecurity and Infrastructure Security Agency (CISA). Secure by Design [Electronic resource]. - Режим доступу: https://www.cisa.gov/securebydesign.

78. Digital Education Action Plan (2021-2027) [Electronic resource] / European Commission. - Режим доступу: https://education.ec.europa.eu/focus-topics/digital-education/action-plan.

79. E-Governance Academy. Information security governance [Electronic resource] // eGovernance.com. - Режим доступу: https://egovernance.com/information-security-governance/

80. European Commission. eEurope 2005: An information society for all. An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002 [Electronic resource] // EUR-Lex. - COM(2002) 263 final. - Brussels, 28.5.2002. - URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF.

81. European Digital Identity Wallet [Electronic resource] // European Commission. Digital Strategy. - URL: https://digital-strategy.ec.europa.eu/en/funding/european-digital-identity-wallet

82. Fiott, D. The virtual front line: How EU tech power can help Ukraine [Electronic resource] // European Council on Foreign Relations (ECFR). - 2024. -

URL: https://ecfr.eu/article/the-virtual-front-line-how-eu-tech-power-can-help-ukraine.

83. Fountain J. E. Building the Virtual State: Information Technology and Institutional Change. Washington, D.C.: Brookings Institution Press, 2001. 251 p.

84. General Data Protection Regulation (GDPR) [Electronic resource]. - URL: https://www.consilium.europa.eu/en/policies/data-protection-regulation/

85. Homburg, V. Understanding E-Government: Information Systems in Public Administration. - London : Routledge, 2008. - 176 p.

86. Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., Scharre, P. Artificial intelligence and international security. - Washington : Center for a New American Security, 2018. - 124 p.

87. Houser, R., Hao, S., Cotton, C., Wang, H. A comprehensive, longitudinal study of government DNS deployment at global scale // 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). - 2022. - P. 193-204.

88. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements [Electronic resource]. - Женева : International Organization for Standardization, 2022. - URL: https://www.iso.org/standard/27001.

89. Karokola, G., Kowalski, S., Yngström, L. Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models // 2011 Information Security for South Africa (ISSA). – Johannesburg, South Africa, 15-17 Aug. 2011. - P. 1-9. - DOI: 10.1109/ISSA.2011.6027525.

90. Kitler, W. National Security: Theory and Practice [Electronic resource]. - Warsaw: Wydawnictwo Towarzystwa Wiedzy Obronnej, 2021. - 278 c. - URL: https://www.researchgate.net/publication/351117604_NATIONAL_SECURITY_THEORY_AND_PRACTICE.

91. Kravchenko, O.; Lytvyn, M.; Melnyk, L. Digital divide and sustainable development of Ukrainian regions [Electronic resource] // Problems and Perspectives in Management. - 2023. - Vol. 21, Iss. 3. - P. 27-41.

92. Matwyshyn, A. M. Harboring Data: Information Security, Law, and the Corporation. - Stanford : Stanford University Press, 2009. - 312 p.

93. Microsoft Security 101 [Electronic resource]. URL: https://www.microsoft.com/en-us/security/business/security-101/

94. Ministry of Digital Transformation of Ukraine; Eastern Europe Foundation. Digital literacy of the population of Ukraine: Survey report [Electronic resource] : [First national digital skills survey]. - 2019. - URL: https://osvita.diia.gov.ua/en/research.

95. Moon M. J. The Evolution of E-Government among Municipalities: Rhetoric or Reality? // Public Administration Review. 2002. Vol. 62, No. 4. P. 424-433. DOI: 10.1111/0033-3352.00196.

96. Norris D. F. Advancing E-Government at the Grassroots: Tortoise or Hare? // Public Administration Review. 2005. Vol. 65, No. 1. P. 64-75. DOI: 10.1111/j.1540-6210.2005.00431.x

97. Obushna N., Korchak N., Evsyukova O., Selivanov S., Larin S. Mechanisms For Preventing Disinformation in Public Administration: Current Issues Management Theory and Studies for Rural Business and Infrastructure Development. 2023. 45(4), 467-476.DOI: https://doi.org/10.15544/mts.2023.45

98. Organisation for Economic Co-operation and Development (OECD). Digital government [Electronic resource]. - URL: https://www.oecd.org/en/topics/digital-government.html.

99. Romaniuk, S. N., Manjikian, M. (Eds.). Routledge Companion to Global Cyber-Security Strategy. - 1st ed. - London : Routledge, 2021. - URL: https://doi.org/10.4324/9780429399718.

100. Ross R., Johnson A., Katzke S., Toth P., Stoneburner G. Guide for Assessing the Security Controls in Federal Information Systems and Organizations:

Building Effective Assessment Plans // NIST Special Publication 800-53A. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

101. Rudenko, O., Zaika, O., Varynskyi, V., Kulchii, I., Myroshnychenko, A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development [Electronic resource] // Edelweiss Applied Science and Technology. - 2024. - Vol. 8, No. 6. - P. 1467-1480. - DOI: https://doi.org/10.55214/25768484.v8i6.2263.

102. Scholl, H. J. E-Government: Information, Technology, and Transformation. - New York : Routledge, 2010. - 320 p.

103. Fyshchuk I., Evsyukova O., Smalskys V. The information and communication support of public authorities in the context of using knowledge management in human resources. Public Policy And Administration. - Vol.20.(2). 2021. P.260- 270. DOI: https://doi.org/10.13165/VPA-21-20-2-09

104. Silva J. M., Ribeiro D., Ramos L. F., Fonte V. A worldwide overview on the information security posture of online public services. 2023. https://doi.org/10.48550/arXiv.2310.01200

105. Skove, S. Estonia discussed sending offensive cyber tools to Ukraine after Russia invaded [Electronic resource] / S. Skove // Defense One. - 2023. - 5 жовтня. - URL: https://www.defenseone.com/threats/2023/10/estonia-sent-offensive-cyber-tools-ukraine-after-russia-invaded/390985/

106. Special Report: Defending Ukraine - Early Lessons from the Cyber War [Electronic resource] / Microsoft. - 2023. - URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/1212211-ms-ukrainespecialreport-fy23-link-update.pdf

107. The EU Cybersecurity Certification Framework [Electronic resource]. - URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

108. Troitiño, D. R., Mazur, V. E-Governance in the European Union. - Cham : Springer, 2023. - 256 p.

109. United Nations Development Programme. Human Development Report 2023/24: Breaking the Gridlock - Reimagining cooperation in a polarized world [Electronic resource] / United Nations Development Programme (UNDP). - New York: UNDP, 2024. - 318 p. - URL: https://hdr.undp.org/system/files/documents/global-report-document/hdr2023-24reporten.pdf

110. United Nations. E-Government Development Index. Department of Economic and Social Affairs. Division for Public Institutions and Digital Governmen. URL: https://publicadministration.un.org/egovkb/en-us/Data-Center

111. United Nations. UN E-Government Survey 2018: Gearing e-government to support transformation towards sustainable and resilient societies [Electronic resource] / United Nations Department of Economic and Social Affairs. – New York: United Nations, 2018. - 270 p. - URL: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

112. United Nations. UN E-Government Survey 2020: Governing in the digital era [Electronic resource] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2020. - 258 p. - URL: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

113. United Nations. UN E-Government Survey 2022: Governing in the digital era [Electronic resource] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2022. - 258 p. - URL: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf

114. United Nations. UN E-Government Survey 2024: Governing in the digital era [Electronic resource] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2024. - 258 p. - URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

115. Viter D., Rudenko O. National Security in the Multi-Domain Environment: Public Administration Issues // Public Administration and Law Review. - 2025. - No. 1(21). - P. 40-49. - DOI: https://doi.org/10.36690/2674-5216-2025-1-40-49.

116. West D. M. Digital Government: Technology and Public Sector Performance. Princeton: Princeton University Press, 2005. 234 p.

117. Whitman, M. E., Mattord, H. J. Principles of information security. – Boston : Cengage Learning, 2021. - 656 p.

118. World Bank. Ukraine e-Government Assessment. 2018. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/379971544700498182/ukraine-e-government-assessment

119. Wu, Chao. Investigation of foundation theory of safety & security complexity // Journal of Safety and Sustainability. - 2024. - Vol. 1, No. 1. - P. 14-25. - DOI: https://doi.org/10.1016/j.jsasus.2023.09.001.

120. Yang, L., Elisa, N., Eliot, N. Privacy and security aspects of E-government in smart cities // Smart cities cybersecurity and privacy / eds. N. Elisa, N. Eliot. - Amsterdam : Elsevier, 2019. - P. 89-102.

121. Kutova M. Adaptation of e-government and information security strategies to new realities. Юність науки - 2024: збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). - Чернігів: НУ «Чернігівська політехніка», 2024. - 1440 с. (С.192)

122. Kutova M. The framework of information security in e-governance system. Науковий журнал «Economic Synergy», випуск 1(11), 2024. - с.20-30. URL: https://doi.org/10.53920/ES-2024-1-2

123. Kutova M. The impact of political and social factors on the development of E-Government and information security in Ukraine Сучасна парадигма публічного управління: Збірник тез VI Міжнародної науково-практичної конференції (14-16 листопада 2024р.) / [За наук. ред. канд. екон.

наук, доц. Стасишина А.В.]. - Електрон. вид. - Львів : ЛНУ імені Івана Франка, 2025. 930 с. (с.83-84).

124. Tulchynska S., Solosich O., Marych M., Marusiak N., Lashuk O. Applied Principles for Ensuring Economic Security of Regional Economic Systems in the Conditions of Digitalization // WSEAS Transactions on Systems and Control. - 2021. - Vol. 16. - P. 600-609. - DOI: https://doi.org/10.37394/23203.2021.16.56

ДОДАТКИ

Додаток А

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Публікації в наукових фахових виданнях України з публічного управління

1. Kutova M. The framework of information security in e-governance system. Науковий журнал «Economic Synergy», випуск 1(11), 2024. - с.20-30. https://doi.org/10.53920/ES-2024-1-2

2. Кутова М. А. Ідентифікація стратегічних напрямів розвитку системи електронного урядування в контексті інформаційної безпеки. Вісник Хмельницького національного університету. Серія: Економічні науки, 2025, №2. - с.60-63. https://doi.org/10.31891/2307-5740-2025-340-8

3. Кутова М. А. Модель стратегічного планування розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки. Вісник Хмельницького національного університету. Серія: Економічні науки, 2025, №3. – с.12-16. https://doi.org/10.31891/2307-5740-2025-342-3(1)-1

Опубліковані праці апробаційного характеру

4. Кутова М. А. Теоретичні аспекти становлення електронного урядування в Україні. Юність науки – 2023: соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей XIII Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 26-27 квітня 2023 р.). – Чернігів: НУ «Чернігівська політехніка», 2023. – 770 с. (с. 213)

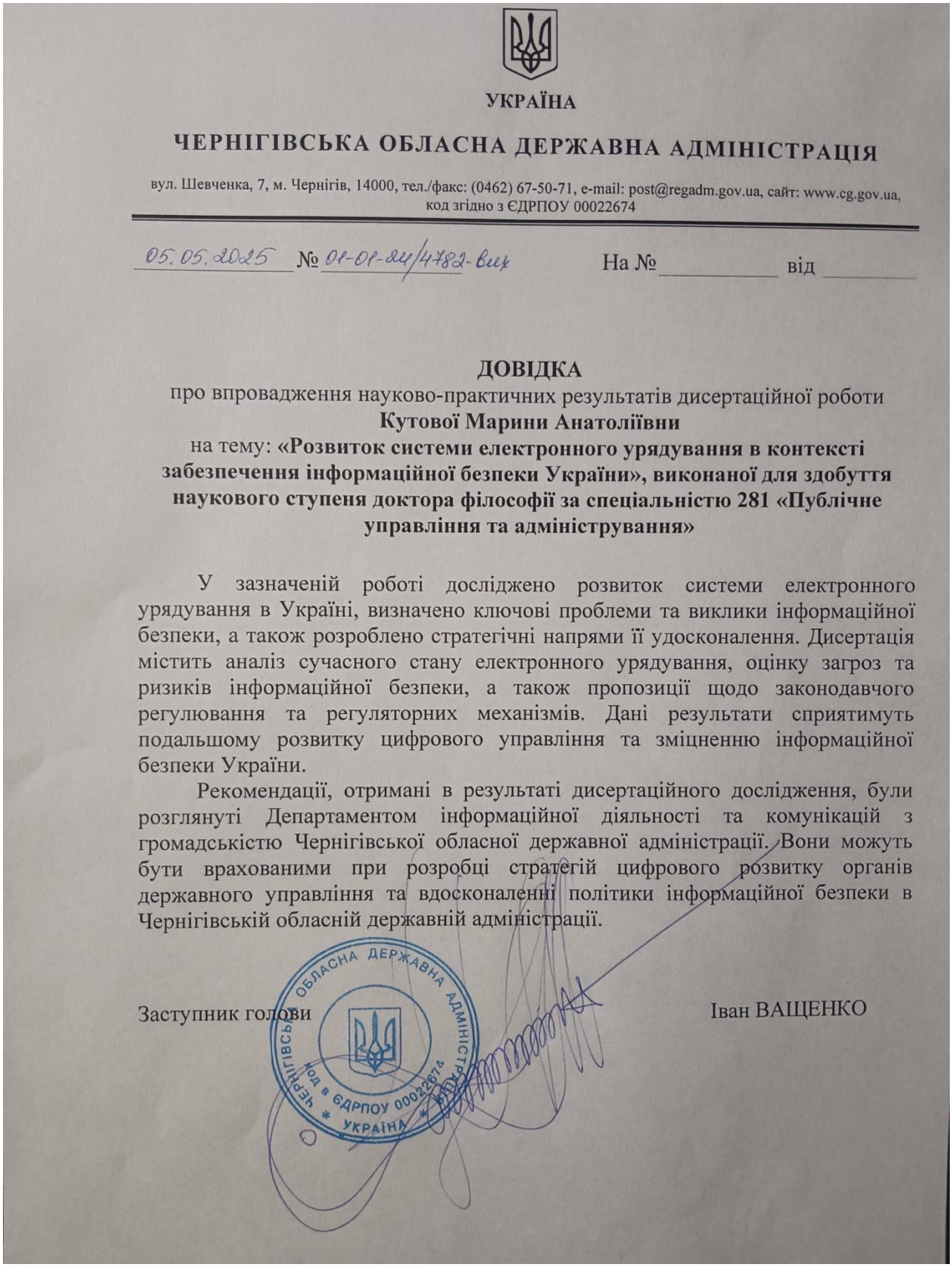
5. Kutova M. Adaptation of e-government and information security strategies to new realities. Юність науки – 2024: збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). – Чернігів: НУ «Чернігівська політехніка», 2024. – 1440 с. (С.192)

6. Kutova M. The impact of political and social factors on the development of E-Government and information security in Ukraine Сучасна парадигма публічного управління : Збірник тез VI Міжнародної науково-практичної конференції (14-16 листопада 2024р.) / [За наук. ред. канд. екон. наук, доц. Стасишина А.В.]. – Електрон. вид. – Львів : ЛНУ імені Івана Франка, 2025. 930 с. (с.83-84)

7. Кутова М.А. Основні загрози та ризики інформаційної безпеки в електронному урядуванні України. International scientific-practical conference “Economics, accounting, finance and management: strategic priorities for development in the context of globalization”: conference proceedings (Tampere, Finland, March 21, 2025). Tampere, Finland: Scholarly Publisher ICSSH, 2025. 37 pages. (с.30-34).

Додаток Б

Довідки про впровадження результатів дисертаційної роботи



УКРАЇНА

ЧЕРНІГІВСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ

вул. Шевченка, 7, м. Чернігів, 14000, тел./факс: (0462) 67-50-71, e-mail: post@regadm.gov.ua, сайт: www.cg.gov.ua, код згідно з ЄДРПОУ 00022674

05.05.2025 № 01-01-24/4782-вих На № _____ від _____

ДОВІДКА

про впровадження науково-практичних результатів дисертаційної роботи **Кутової Марини Анатоліївни** на тему: **«Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України», виконаної для здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування»**

У зазначеній роботі досліджено розвиток системи електронного урядування в Україні, визначено ключові проблеми та виклики інформаційної безпеки, а також розроблено стратегічні напрями її удосконалення. Дисертація містить аналіз сучасного стану електронного урядування, оцінку загроз та ризиків інформаційної безпеки, а також пропозиції щодо законодавчого регулювання та регуляторних механізмів. Дані результати сприятимуть подальшому розвитку цифрового управління та зміцненню інформаційної безпеки України.

Рекомендації, отримані в результаті дисертаційного дослідження, були розглянуті Департаментом інформаційної діяльності та комунікацій з громадськістю Чернігівської обласної державної адміністрації. Вони можуть бути врахованими при розробці стратегій цифрового розвитку органів державного управління та вдосконаленні політики інформаційної безпеки в Чернігівській обласній державній адміністрації.

ЧЕРНІГІВСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ Код в ЄДРПОУ 00022674 УКРАЇНА

Заступник голови Іван ВАЩЕНКО

УКРАЇНА
ІВАНІВСЬКА СІЛЬСЬКА РАДА
ЧЕРНІГІВСЬКОГО РАЙОНУ ЧЕРНІГІВСЬКОЇ ОБЛАСТІ
вул. Дружби, 33Б, с. Іванівка, 15562 тел. 0960848939 e-mail:iv_cnap@ukr.netS ivanivska_silska_rada@ukr.net, код ЄДРПОУ 04412751

28.04.2025 р. № 305

ДОВІДКА
про впровадження науково-практичних результатів дисертаційної роботи Кутової Марини Анатоліївни
на тему: «Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України», виконаної для здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування»

У дисертаційній роботі досліджено проблематику цифрового врядування на місцевому рівні, зокрема питання безпечного надання електронних адміністративних послуг у територіальних громадах, механізми підвищення ефективності функціонування електронних сервісів та вдосконалення захисту персональних даних громадян.

Рекомендації, сформовані в рамках дисертаційного дослідження, були враховані Центром надання адміністративних послуг Іванівської сільської ради при впровадженні цифрових рішень для спрощення надання адміністративних послуг. Зокрема, застосовані підходи сприяли оптимізації документообігу у процесі обслуговування населення. Використання отриманих наукових напрацювань сприяє підвищенню якості надання адміністративних послуг у громаді, розширенню доступу до електронних сервісів та забезпеченню надійного рівня кіберзахисту.

Начальник ЦНАП **С.С.Петренко**

УКРАЇНА
ЧЕРНІГІВСЬКА МІСЬКА РАДА
УПРАВЛІННЯ АДМІНІСТРАТИВНИХ ПОСЛУГ
проспект Левка Лукяненка, 20-А, м. Чернігів, 14032, тел./факс 651-910, ЄДРПОУ 38271176,
e-mail: cnap@chernigiv-rada.gov.ua

_____ № _____ на № _____

ДОВІДКА
про впровадження науково-практичних результатів дисертаційної роботи Кутової Марини Анатоліївни
на тему: «Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України»,
виконаної для здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування»

У дисертаційній роботі досліджено розвиток системи електронного урядування, зокрема питання ефективної цифрової взаємодії між органами державної влади та громадянами, а також виклики інформаційної безпеки. Запропоновано методичні підходи до покращення інформаційної безпеки в рамках надання електронних адміністративних послуг.

Практичні рекомендації, сформульовані в результаті дисертаційного дослідження, були використані Управлінням адміністративних послуг Чернігівської міської ради при модернізації інформаційних систем надання адміністративних послуг, підвищенні рівня кіберзахисту та вдосконаленні механізмів електронної ідентифікації громадян. Впроваджені заходи сприяли оптимізації процесів обслуговування громадян, зменшенню бюрократичного навантаження та підвищенню ефективності взаємодії населення з органами місцевого самоврядування.

Зазначені результати мають значний практичний ефект і продовжують використовуватися у процесі цифрової трансформації міських адміністративних послуг.

Заступник начальника управління –
начальник відділу - державний реєстратор
відділу державної реєстрації юридичних осіб
та фізичних осіб підприємців Олексій ГОЛОВАН

(0462) 65-19-09

№ 2354 від 22.05.2025

Управління адміністративних послуг
Чернігівської міської ради

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

вул. Шевченка, 95, Чернігів, 14035, Україна

тел. +38(0462) 665-103;
факс +38(0462) 665-105
E-mail: cstu@stu.cn.ua
www.stu.cn.ua
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

CHERNIHIV POLYTECHNIC NATIONAL UNIVERSITY

95, Shevchenko str., Chernihiv, 14035, Ukraine

07.05.2025 № 202/08-997/вс

На № _____ від _____

ДОВІДКА
про впровадження результатів дисертаційної роботи
Кутової Марини Анатоліївни
на тему : *«Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України»*

Основні положення та результати дисертаційного дослідження Кутової Марини Анатоліївни на тему: «Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України», використані при виконанні науково-дослідної роботи Національного університету «Чернігівська політехніка» МОН України, зокрема: «Механізми державного управління регіональним розвитком в умовах переформатування владних відносин» (номер державної реєстрації 0120U105292), у межах якої здобувачем розроблено механізм реалізації державної регіональної політики у сфері електронного урядування, який, на відміну від існуючих підходів, враховує територіальну нерівномірність розвитку цифрової інфраструктури, різний рівень доступності електронних послуг для населення, а також регіональні відмінності у ризиках та загрозах інформаційній безпеці. Запропоновані зміни спрямовані на створення цілісної та безпечної системи електронного врядування, побудованої на засадах цифрової інклюзії, зміцнення інституційної спроможності місцевих органів влади та впровадження багаторівневої системи управління, яка забезпечує координацію між центральними та регіональними структурами.

Система управління якістю сертифікована за ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT)

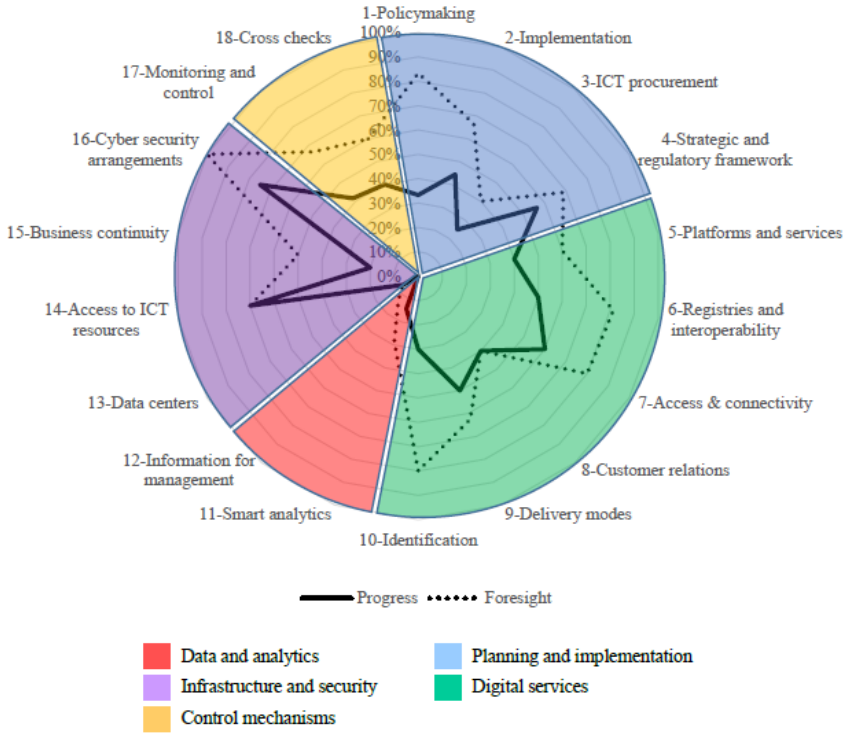
The quality management system is certified according to the ISO 9001:2015

Варто зазначити, що результати наукового дослідження Кутової Марини Анатоліївни містять наукову новизну, практичний інтерес та доцільність впровадження в навчальний процес кафедри менеджменту та адміністрування при викладанні дисциплін «Публічне управління національною та державною безпекою» (доктор філософії), «Інформаційна політика та електронне врядування» (освітній ступінь магістр). В межах змістовного модуля «Організаційно-методичні основи створення та функціонування системи електронного урядування» були запропоновані питання дослідження функціонування системи електронного урядування для оцінки ризиків і загроз інформаційної безпеки.

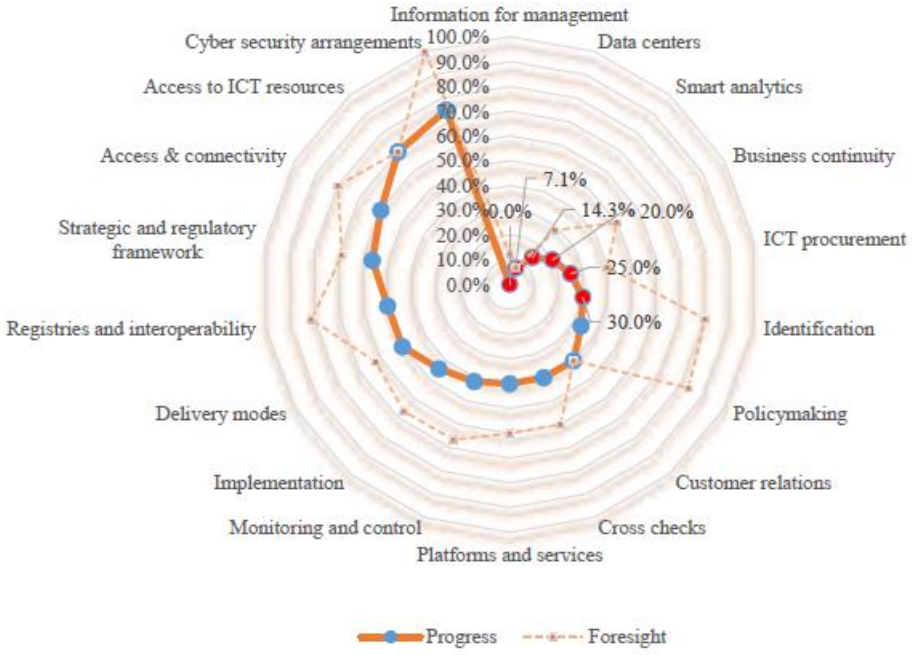
Проректор з наукової роботи
НУ «Чернігівська політехніка»,
к.т.н., доцент Анатолій ПРИСТУПА

Додаток В

Результати оцінки електронного урядування України здійсненого Світовим Банком



Підсумок оцінки eGGO за вимірами та напрямками



Виміри оцінювання eGGO за пріоритетами

Додаток Г

Індекс цифрової трансформації України за даними Мінціфри України

Назва області	Значення Індексу
Загалом для України	0,632
Дніпропетровська	0,908
Львівська	0,891
Полтавська	0,833
Волинська	0,831
Тернопільська	0,827
Харківська**	0,787
Одеська	0,785
Вінницька	0,777
Закарпатська	0,732
Рівненська	0,727
Івано-Франківська	0,685
Київська	0,684

Назва області	Значення Індексу
Черкаська	0,672
Хмельницька	0,620
Житомирська	0,560
Чернігівська	0,553
Чернівецька	0,546
Кіровоградська	0,531
Миколаївська**	0,441
Луганська*	0,404
Донецька**	0,359
Херсонська**	0,316
Запорізька**	0,289
Сумська	0,178
Автономна Республіка Крим***	0,000

Додаток Д

Активність на вебплатформі Дія. Освіт за даними Мінціфри України