

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

Кваліфікаційна наукова  
праця на правах рукопису

**ПОПОВ ОЛЕКСАНДР ПАВЛОВИЧ**

УДК 35.075.5-027.555:004.67(043)

**ДИСЕРТАЦІЯ**

**МЕХАНІЗМИ ЦИФРОВОЇ ВЗАЄМОДІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ  
В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ**

281 Публічне управління та адміністрування

28 Публічне управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

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

\_\_\_\_\_ О. П. Попов

Науковий керівник: Сурай Інна Геннадіївна, доктор наук з державного  
управління, професор

м. Івано-Франківськ – 2026

## АНОТАЦІЯ

*Попов О. П.* Механізми цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування. – Карпатський національний університет імені Василя Стефаника, Івано-Франківськ, Міністерство освіти і науки України, м. Івано-Франківськ, 2026.

У дисертаційній роботі узагальнено науково-теоретичні основи та здійснено теоретико-методологічне обґрунтування механізмів цифрової взаємодії органів публічної влади, розроблено практичні рекомендації щодо удосконалення їх функціонування в умовах розвитку електронного урядування.

У дисертації окреслено дискурсне поле проблем цифрової взаємодії, що дозволило виокремити багаторівневу природу цього явища, яке охоплює правові, організаційні, технологічні та соціально-комунікативні аспекти. Проаналізовано еволюцію підходів до цифровізації публічного управління, починаючи від автоматизації адміністративних процесів і завершуючи сучасними концепціями управління на основі даних (data-driven governance), орієнтованого на громадян (citizen-centric governance) та стійкого до ризиків і криз (resilient governance), що передбачає використання цифрових технологій для прийняття рішень на основі даних, підвищення участі та задоволеності громадян, а також забезпечення безперервності та надійності публічних сервісів у складних умовах. Встановлено дві ключові лінії наукового пошуку: техніко-технологічну (архітектура інформаційних систем, кіберзахист, стандартизація) та соціо-гуманітарну (людиноцентричність, прозорість, інклюзивність, громадська участь), що взаємодіють із сучасними теоріями електронної демократії та соціального капіталу.

В рамках теоретичного аналізу уточнено категоріально-понятійний апарат: визначено взаємозв'язки між поняттями «електронне урядування», «цифрова

взаємодія», «інтероперабельність» та «механізми цифрової взаємодії». Показано, що електронне урядування формує загальну модель управління, цифрова взаємодія виступає ключовим механізмом реалізації, а інтероперабельність – техніко-організаційною основою, що забезпечує функціональність і сталість цього механізму. Особлива увага приділена інтеграції структурних (право, інституції, технології) і функціональних (процедури, стандарти, практики) компонентів механізмів цифрової взаємодії. Виділено технологічний, комунікативний, правовий та економічний напрями розвитку цих категорій.

Емпірична частина дослідження охоплює аналіз стану інтероперабельності інформаційних систем органів публічної влади в Україні. Виявлено досягнення, такі як запуск державної шини обміну «Трембіта», інтеграція з платформою «Дія», уніфікація форматів даних та створення реєстру метаданих. Водночас встановлено наявність бар'єрів: цифрова фрагментація, обмежені повноваження центрального координатора (Міністерства цифрової трансформації), нестача семантичних стандартів, кадрова прогалина та ризики кібербезпеки. Порівняльний аналіз із зарубіжними моделями (ЄС, Велика Британія, скандинавські країни) підкреслив необхідність мультимірної інтероперабельності (технічної, семантичної, організаційної, юридичної та політичної).

Окреслено комплекс безпекових викликів, пов'язаних із цифровою взаємодією органів публічної влади, що включає технічні, організаційні, правові та соціальні аспекти. Зокрема, проаналізовано загрози інформаційній безпеці, ризики несанкціонованого доступу до державних інформаційних ресурсів, потенційні кіберзлочини та недоліки у захисті персональних даних громадян. Встановлено, що ефективне подолання цих викликів потребує інтегрованого інституційно-функціонального підходу, який поєднує нормативно-правові, організаційні та технологічні заходи.

Обґрунтовано вихідні положення щодо відстеження кіберзагроз у системі цифрової взаємодії органів публічної влади, які надають електронні державні послуги та є потенційно вразливими через великі обсяги персональних даних,

фінансову інформацію та критичну інфраструктуру. Запропоновано застосування розробленої Індикативної панелі відстеження кіберзагроз як ефективного інструменту систематизації процесів моніторингу, аналізу та реагування на загрози. Панель забезпечує централізовану структуру відстеження кіберризиків, дозволяє виявляти слабкі місця в системах захисту, оперативно реагувати на інциденти та впроваджувати превентивні заходи для мінімізації ризиків. Визначено ключові показники панелі, серед яких кількість невдалих спроб авторизації, обсяг аномального трафіку, виявлені вразливості, несанкціоновані зміни конфігурації серверів, інциденти втрати даних та задоволеність користувачів електронними послугами. Для кожного показника передбачено частоту моніторингу, метод збору даних, відповідальних осіб, поріг тривоги та конкретні дії при його перевищенні. Застосування панелі дозволяє підвищити ефективність управління кіберризиками, сприяє розвитку культури інформаційної безпеки серед публічних службовців, підвищує прозорість і довіру громадян до цифрових платформ, створюючи науково обґрунтовану основу для безпечного та стійкого розвитку електронного урядування.

Окрему увагу приділено підвищенню цифрової компетентності публічних службовців через системне навчання, розробку стандартів цифрової обізнаності, тренінги з кібергігієни та практичні інструктажі щодо роботи із захищеними інформаційними системами. Підкреслено важливість поєднання технічних рішень із формуванням культури безпеки серед службовців та підвищенням їхньої здатності ухвалювати рішення в умовах інформаційних ризиків.

Науково обґрунтовано архітектурну модель механізмів цифрової взаємодії органів публічної влади, яка інтегрує п'ять взаємопов'язаних компонент. Цільово-функціональна компонента (організаційна архітектура), включає управлінські функції, адміністративні процеси та стратегічні пріоритети, забезпечуючи цілісність і координацію діяльності органів влади. Інформаційно-комунікативна компонента (інформаційна архітектура), передбачає стандартизацію, обіг та повторне використання даних через національні платформи, що гарантує ефективний обмін інформацією між суб'єктами

цифрової взаємодії. Сервісно-інтеграційна компонента (прикладна архітектура) охоплює цифрові сервіси, API, реєстрові шлюзи та електронний документообіг, забезпечуючи взаємодію між інформаційними системами та користувачами. Інфраструктурно-технологічна компонента (технічна архітектура), пов'язується із використанням хмарних і туманних платформ, серверних рішень та заходів кіберзахисту, створюючи надійну технологічну основу для цифрових процесів. Кадрово-ресурсна компонента (архітектура людського потенціалу) спрямована на розвиток цифрових компетенцій державних службовців та формування цифрової культури у публічному управлінні.

Запропоновано комплексну методику оцінювання функціонування механізмів цифрової взаємодії у вигляді багатовимірної матриці моніторингу, що поєднує контрольні, оцінні та організаційно-технічні інструменти, інтегруючи різнотипні шкали (кількісні, бінарні, якісні, агреговані) та мультиджерельні дані (реєстри, системні логи, внутрішні звіти, опитування користувачів). Методика дозволяє одночасно оцінювати технічну ефективність, організаційні спроможності, правові та кадрові аспекти, кібербезпеку і рівень громадської довіри, що формує основу для розробки політики, заснованої на доказах (evidence-based policy): управлінських рішень, які спираються на надійні дані, факти та результати наукових досліджень, а не лише на інтуїцію чи традиційні практики, що підвищує їх ефективність та передбачуваність.

Висновки та рекомендації дисертаційного дослідження спрямовані на подолання існуючих бар'єрів і підвищення ефективності цифрової взаємодії: інституційна консолідація управління інтегрованістю, формалізація посад CDTO (Chief Digital Transformation Officer, заступник керівника з цифровізації), масштабування цифрових офісів, розвиток національної хмарної платформи, впровадження етичних стандартів застосування штучного інтелекту (ШІ), регламентація кібербезпеки та стимулювання професійного розвитку публічних службовців.

Отримані результати становлять вагомий внесок у розвиток теорії та практики публічного управління, зокрема у сфері механізмів цифрової взаємодії

органів публічної влади в умовах розвитку електронного урядування, і можуть бути використані для вдосконалення політик цифрової трансформації, підвищення ефективності роботи органів публічної влади, забезпечення цифрової інклюзії через формування партисипативного середовища, орієнтованого на принципи прозорості, підзвітності та людиноцентричності.

**Ключові слова:** публічне управління, механізми, електронне урядування, цифрові технології, цифровізація публічних (державних) послуг, цифрові платформи, цифрова взаємодія, цифрова трансформація, інформаційна безпека (кібербезпека), органи публічної влади, інтероперабельність інформаційних систем, електронні послуги (е-послуги), адміністративні послуги, публічні послуги, зарубіжний досвід.

## ABSTRACT

*Oleksandr Popov.* Mechanisms of Digital Interaction of Public Authorities in the Context of E-Government Development. – Manuscript-based qualification research paper.

Thesis for the degree of Doctor of Philosophy in 28 Public Management and Administration, specialty 281 Public Management and Administration. Vasyl Stefanyk Carpathian National University of the Ministry of Education and Science of Ukraine, Ivano-Frankivsk, 2026.

The dissertation generalizes the scientific and theoretical foundations, provides a theoretical and methodological justification of the mechanisms of digital interaction of public authorities, and develops practical recommendations for improving their functioning in the context of e-government development.

The study examines the discursive field of digital interaction issues, revealing the multi-level nature of this phenomenon, which encompasses legal, organizational, technological, and socio-communicative dimensions. The evolution of approaches to digitalization in public administration has been analyzed, starting from process automation and culminating in modern concepts of data-driven governance, citizen-centric governance, and resilient governance, which involve the use of digital

technologies for evidence-based decision-making, enhancing citizen participation and satisfaction, and ensuring continuity and reliability of public services under complex conditions. Two key lines of scientific inquiry were identified: a techno-technological line, covering information system architecture, cybersecurity, and standardization, and a socio-humanitarian line, emphasizing human-centeredness, transparency, inclusiveness, and civic engagement, which interact with contemporary theories of e-democracy and social capital.

Within the theoretical analysis, the conceptual framework was refined by clarifying the relationships between “e-government,” “digital interaction,” “interoperability,” and “mechanisms of digital interaction.” E-government is shown to form the overarching management model, digital interaction serves as the key implementation mechanism, and interoperability provides the technical and organizational basis ensuring the functionality and sustainability of this mechanism. Special attention was paid to integrating structural components (law, institutions, technologies) with functional components (procedures, standards, practices) of digital interaction mechanisms, highlighting technological, communicative, legal, and economic dimensions of their development.

The empirical part analyzes the state of interoperability of information systems of public authorities in Ukraine. Achievements include the launch of the national data exchange bus “Trembita,” integration with the “Diia” platform, data format unification, and creation of a metadata registry. However, barriers such as digital fragmentation, limited powers of the central coordinator (Ministry of Digital Transformation), lack of semantic standards, human resource gaps, and cybersecurity risks were identified. Comparative analysis with foreign models (EU, UK, Nordic countries) emphasized the need for multidimensional interoperability (technical, semantic, organizational, legal, and political).

The study explores a comprehensive range of security challenges related to digital interaction, including technical, organizational, legal, and social aspects. Information security threats, risks of unauthorized access to state information resources, potential cybercrimes, and weaknesses in citizen personal data protection

were analyzed. It was determined that effectively addressing these challenges requires an integrated institutional and functional approach combining regulatory, organizational, and technological measures.

The dissertation substantiates the principles of cyber threat monitoring in digital interaction systems of public authorities providing electronic public services, which are potentially vulnerable due to large volumes of personal, financial, and critical infrastructure data. The proposed Indicative Cyber Threat Monitoring Panel serves as an effective tool for systematizing monitoring, analysis, and response processes, providing a centralized structure for tracking cyber risks, identifying weaknesses in protection systems, responding to incidents promptly, and implementing preventive measures to minimize risks. Key indicators include the number of failed authorizations, anomalous traffic volume, detected vulnerabilities, unauthorized server configuration changes, data loss incidents, and user satisfaction with e-services. For each indicator, the panel specifies monitoring frequency, data collection methods, responsible personnel, alert thresholds, and actions upon exceeding these thresholds. The panel enhances cyber risk management, fosters a culture of information security among public servants, and increases transparency and citizen trust in digital platforms, creating a scientifically grounded basis for safe and sustainable e-government development.

Particular attention is given to improving the digital competencies of public servants through systematic training, development of digital literacy standards, cybersecurity hygiene exercises, and practical guidance for operating secure information systems. The integration of technical solutions with the cultivation of a security culture and the enhancement of decision-making capabilities under information risk conditions is emphasized.

The dissertation proposes an architectural model of digital interaction mechanisms of public authorities, integrating five interrelated components. The goal-functional component (organizational architecture) includes management functions, administrative processes, and strategic priorities, ensuring coherence and coordination. The information-communication component (information architecture) provides data

standardization, circulation, and reuse through national platforms, guaranteeing effective information exchange among digital interaction entities. The service-integration component (application architecture) covers digital services, APIs, registry gateways, and electronic document management, ensuring interaction between information systems and users. The infrastructure-technology component (technical architecture) incorporates cloud and fog platforms, server solutions, and cybersecurity measures, creating a reliable technological foundation. The human-resources component (human potential architecture) focuses on developing digital competencies of public servants and fostering a digital culture in public administration.

A comprehensive methodology for assessing digital interaction mechanisms is proposed in the form of a multidimensional monitoring matrix, combining control, evaluation, and organizational-technical instruments, integrating diverse scales (quantitative, binary, qualitative, aggregated) and multi-source data (registries, system logs, internal reports, user surveys). The methodology simultaneously evaluates technical efficiency, organizational capacity, legal and human resource aspects, cybersecurity, and public trust, forming a basis for evidence-based policy, i.e., decision-making grounded in reliable data, facts, and scientific research rather than intuition or traditional practices, enhancing effectiveness and predictability.

The dissertation's conclusions and recommendations aim to overcome existing barriers and enhance digital interaction effectiveness: institutional consolidation of interoperability management, formalization of CDTO positions, scaling digital offices, development of a national cloud platform, implementation of ethical AI standards, cybersecurity regulation, and professional development incentives for public servants.

The obtained results make a significant contribution to the development of theory and practice of public management, particularly in mechanisms of digital interaction of public authorities in the context of e-government development, and can be applied to improve digital transformation policies, enhance operational efficiency of public authorities, and ensure digital inclusion through participatory environments based on transparency, accountability, and human-centered principles.

**Key words:** public management, mechanisms, e-government, digital technologies, digitalisation of public services, digital platforms, digital interaction, digital transformation, information security (cybersecurity), public authorities, interoperability of information systems, electronic services (e-services), administrative services, public services, foreign experience.

## СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

### Статті в наукових фахових виданнях України категорії Б:

1. Попов О.П. Історичні засади розвитку інформаційних систем, цифрової сумісності у взаємодії органів публічної влади. *Інвестиції: практика та досвід*. 2023. № 16. С. 233-238.

DOI: <http://doi.org/10.32702/2306-6814.2023.16.233>

URL: <https://nayka.com.ua/index.php/investplan/article/view/1953/1974>

2. Попов О.П. Дискурсне поле цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. *Електронний журнал «Державне управління: удосконалення та розвиток»*. 2023, № 11.

DOI: <http://doi.org/10.32702/2307-2156.2023.11.25>

URL: <https://www.nayka.com.ua/index.php/dy/article/view/2444>

3. Попов О.П. Безпекові аспекти цифрової взаємодії у системі органів публічної влади в Україні. *Інвестиції: практика та досвід*. 2024. № 16. С. 309-314.

DOI: <http://doi.org/10.32702/2306-6814.2024.16.309>

URL: <https://www.nayka.com.ua/index.php/investplan/article/view/4396/4431>

4. Попов О.П. Цифрова взаємодія інформаційних систем органів публічної влади: аналіз світових практик. *Актуальні питання у сучасній науці*. 2025. № 1(31). С. 339-347.

DOI: [https://doi.org/10.52058/2786-6300-2025-1\(31\)-339-347](https://doi.org/10.52058/2786-6300-2025-1(31)-339-347)

URL: <http://perspectives.pp.ua/index.php/sn/article/view/18792/18817>

**Статті у періодичних наукових виданнях інших держав, які входять до  
Організації економічного співробітництва та розвитку та/або  
Європейського Союзу, з наукового напрямку, за яким підготовлено  
дисертацію здобувача:**

5. Popov O. Analysis of terms and concepts «electronic government», «digital interaction of public authorities», «information systems». Sciences of Europe. Praha, 2022. № 107. P. 112-115.

DOI: <https://doi.org/10.5281/zenodo.7479780>

URL: <https://www.europe-science.com/wp-content/uploads/2022/12/Sciences-of-Europe-No-107-2022.pdf>

**Публікації, які засвідчують апробацію матеріалів дисертації:**

6. Oleksandr Popov. Implementation of digital interaction in public administration. “Science And Innovation Of Modern World”: materials of the I International Scientific and Practical Conference (London, United Kingdom. 28-30 September, 2022) P. 354-357.

URL: <https://sci-conf.com.ua/wp-content/uploads/2022/09/SCIENCE-AND-INNOVATION-OF-MODERN-WORLD-28-30.09.22.pdf>

7. Oleksandr Popov. Digital interaction of public authorities. “Science And Technology: Problems, Prospects And Innovations” : materials of the I International Scientific and Practical Conference (Osaka, Japan. 19-21 October, 2022) P. 338-341.

URL: <https://sci-conf.com.ua/wp-content/uploads/2022/10/SCIENCE-AND-TECHNOLOGY-PROBLEMS-PROSPECTS-AND-INNOVATIONS-19-21.10.22.pdf>

8. Oleksandr Popov. Digitalization of the activities of public authorities. “Priority directions of science development” : materials of the V International Scientific and Practical Conference (Hamburg, Germany. 6-8 February 2023) P. 278-280.

URL: <https://eu-conf.com/wp-content/uploads/2023/02/Priority-directions-of-science-development.pdf>

9. Oleksandr Popov. E-democracy as a tool for optimizing the interaction

between government and citizens in the conditions of electronic government. «Scientific progress: innovations, achievements and prospects» : materials of the VII International Scientific and Practical Conference (Munich, Germany. 3-4 April 2023) P. 400-404.

URL: <https://sci-conf.com.ua/wp-content/uploads/2023/04/SCIENTIFIC-PROGRESS-INNOVATIONS-ACHIEVEMENTS-AND-PROSPECTS-3-5.04.23.pdf>

10. Олександр Попов. Практика впровадження електронного урядування у Великобританії. Матеріали II міжнародної наукової конференції «Education and science of today: intersectoral issues and development of sciences» (м. Кембридж, Сполучене Королівство Великої Британії і Північної Ірландії, 18 серпня 2023) P. 55-57.

URL:<https://archive.logos-science.com/index.php/conference-proceedings/issue/view/14/14>

11. Oleksandr Popov. International standards of digital interaction of public authorities of Ukraine in the context of the development of electronic governance. «Science and society: modern trends in a changing world»: materials of the IX International Scientific and Practical Conference (Vienna, Austria, August 5-7, 2024) P. 216-219.

URL:<https://sci-conf.com.ua/wp-content/uploads/2024/08/SCIENCE-AND-SOCIETY.-MODERN-TRENDS-IN-A-CHANGING-WORLD-5-7.08.24.pdf>

12. Oleksandr Popov. Global trends in implementing innovative technologies into e-governance practices. «Scientific achievements of contemporary society»: materials of the I International Scientific and Practical Conference (London, United Kingdom. August 15-17, 2024) P. 328-331.

URL:<https://sci-conf.com.ua/wp-content/uploads/2024/08/SCIENTIFIC-ACHIEVEMENTS-OF-CONTEMPORARY-SOCIETY-15-17.08.24.pdf>

## ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	15
ВСТУП	16
РОЗДІЛ 1. ТЕОРЕТИКО-ІСТОРИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМ ЦИФРОВОЇ ВЗАЄМОДІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ	28
1.1 Аналіз ключових понять дослідження, їх взаємозв'язок із суміжними термінами	28
1.2 Історичні основи розвитку інформаційних систем, цифрової сумісності та взаємодії органів публічної влади	48
1.3 Стан наукових досліджень проблем цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування	60
РОЗДІЛ 2. ОСОБЛИВОСТІ МЕХАНІЗМІВ ЦИФРОВОЇ ВЗАЄМОДІЇ ТА ІНТЕРОПЕРАБЕЛЬНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ ТА СВІТІ	733
2.1 Нормативно-правовий та організаційний механізми цифрової взаємодії органів публічної влади України в умовах розвитку електронного урядування	733
2.2. Характеристика механізмів цифрової взаємодії та інтеперабельності інформаційних систем органів публічної влади у провідних країнах світу	911
2.3 Безпекові виклики та можливості цифрової взаємодії органів публічної влади в Україні	1033
РОЗДІЛ 3. ШЛЯХИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЦИФРОВОЇ ВЗАЄМОДІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ	125

3.1 Запровадження інтеперабельності інформаційних систем органів публічної влади як чинник удосконалення механізмів цифрової взаємодії	125
3.2. Матриця моніторингу функціонування механізмів цифрової взаємодії органів публічної влади як оціночна методика у досліджуваній сфері	146
3.3. Пропозиції та рекомендації щодо пріоритетних напрямів удосконалення механізмів цифрової взаємодії органів публічної влади для ефективного розвитку електронного урядування	165
ВИСНОВКИ	186
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	196
ДОДАТКИ	222

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,  
СКОРОЧЕНЬ І ТЕРМІНІВ**

ООН	–	Організація Об'єднаних Націй
ОЕСР	–	Організації економічного співробітництва та розвитку
ЄС	–	Європейський Союз
ВР	–	Верховна рада України
ЄС	–	Європейський Союз
ІКТ	–	Інформаційно-комунікативні технології
ІС	–	Інформаційна система
КМУ	–	Кабінет Міністрів України
ЦОВВ	–	Центральний орган виконавчої влади
Мінцифри	–	Міністерство цифрової трансформації України
ОДА	–	Обласна державна адміністрація
РДА	–	Районна державна адміністрація
ISO	–	Міжнародна організація зі стандартизації
OAS	–	Організація американських держав

## ВСТУП

*Актуальність теми дослідження.* Україна, визначивши європейський вектор свого цивілізаційного та інституційного розвитку, стратегічно пов'язує національну траєкторію розвитку електронного урядування та технологічних змін з інтеграцією у спільний цифровий простір Європейського Союзу. У «Європейській декларації про цифрові права та принципи для цифрового десятиліття» (European Declaration on Digital Rights and Principles, 2022) закріплено засадничі орієнтири цифровізації, серед яких провідне місце посідає принцип людиноцентризму, що ґрунтується на універсальних цінностях, основних правах і свободах людини та спрямований на забезпечення справедливого й інклюзивного цифрового середовища. Декларація гарантує право кожної особи на доступ до базових цифрових державних послуг, участь у публічному цифровому просторі, а також на реалізацію свободи вираження поглядів, зборів та асоціацій у цифровому середовищі. Водночас стратегічні ініціативи ЄС: «ЄС наступного покоління» (NextGenerationEU, 2021), «Шлях до цифрового десятиліття» (Path to the Digital Decade, 2022), а також «Акт про інтероперабельну Європу» (Interoperable Europe Act, 2022) формують нову архітектоніку цифрової взаємодії, у межах якої пріоритетами стають інтероперабельність інформаційних систем, прозорість цифрових процесів, безпека даних та стійкість цифрової інфраструктури.

Цілком очевидно, що для України розвиток механізмів цифрової взаємодії органів публічної влади є визначальним чинником модернізації національної системи електронного урядування. Саме від якості організації міжвідомчого обміну даними, узгодженості цифрових платформ, стандартизації процедур та рівня інституційної координації залежить результативність діяльності органів публічної влади та рівень довіри громадян до держави. Цифрова взаємодія сьогодні постає не лише як технологічна категорія, а як комплексний управлінський інструмент, що дозволяє переосмислити парадигму публічного управління, спрямувавши її на принципи відкритості, підзвітності та інклюзивності.

Сучасний стан цифрової трансформації в Україні характеризується суперечливими тенденціями. З одного боку, суспільство дедалі більше потребує швидких, зручних та стандартизованих адміністративних послуг, інтегрованих у єдиний цифровий простір, з іншого – у національній практиці залишаються проблеми цифрової фрагментації, низького рівня інтероперабельності інформаційних систем, дублювання функцій у правовому полі, а також обмеженої кадрової та інституційної спроможності органів публічної влади. Такі дисбаланси істотно ускладнюють побудову цілісної цифрової архітектури електронного урядування та створюють бар'єри для інтеграції України в європейський цифровий простір.

Відтак, удосконалення механізмів цифрової взаємодії постає як першочергове завдання державної політики у сфері електронного урядування. Йдеться не лише про забезпечення технічної сумісності інформаційних систем, але й про розробку інституційно сталих та нормативно врегульованих механізмів, здатних гарантувати прозорий, безпечний і безперервний міжвідомчий обмін даними.

Важливо наголосити, що сучасна цифрова взаємодія органів публічної влади має орієнтуватися на глобально усталені управлінські парадигми: *data-driven governance* (управління на основі даних), *citizen-centric governance* (людиноцентричне управління) та *resilient governance* (стійке управління). Особливого значення набуває імплементація положень Акта про інтероперабельну Європу, що передбачає створення постійного координаційного органу: Ради з питань інтероперабельної Європи (*Interoperable Europe Board*), наділеного повноваженнями з розробки єдиних стандартів цифрової взаємодії та поширення кращих практик між країнами-членами ЄС. Для України адаптація цих положень відкриває можливість подолати нормативно-правову та технологічну фрагментарність, сформувати комплексну систему управління міжвідомчим обміном даними та інтегрувати національну архітектуру електронного урядування в сучасне європейське цифрове середовище.

Таким чином, актуальність дослідження обумовлена поєднанням трьох взаємопов'язаних чинників: необхідністю створення цілісної архітектури цифрової взаємодії органів публічної влади на засадах інтеоперабельності, прозорості та безпеки; потребою подолання суперечностей і фрагментарних процесів у національній системі електронного урядування; інтеграційними зобов'язаннями України, які визначають необхідність гармонізації вітчизняних цифрових механізмів із європейськими стандартами.

Аналіз останніх досліджень і публікацій засвідчує, що проблеми розвитку електронного урядування та цифрової взаємодії органів публічної влади є одним із провідних напрямів сучасної науки публічного управління. Дослідники концентрують увагу на різних аспектах проблематики. Так, питання термінологічного апарату проблем цифрової взаємодії висвітлено у працях С. Скорика, Н. Рябоконт [73], К. Сімакова та ін. [74]. Теоретико-методологічні підходи до цифрової трансформації публічного управління окреслено у наукових роботах П. Данліві та Г. Маргеттс [46], Ю. Мохової [76], Г. та М. Разумеїв [75], М. Нагорняка, О. Дегтяра, І. П'ятничук, О. Пархоменко-Куцевіл, Т. Маматової, І. Сурай. Питання інституційного забезпечення та правових засад розвитку електронного урядування проаналізовано в дослідженнях О. Романчука [78], С. Чернецького [77]. У працях зарубіжних учених, зокрема М. Техедо-Ромеро [3], Д. О'Коннора [23], С. Ходаппа [53], акцент зроблено на вивченні інноваційних моделей цифрових платформ, питаннях інтеоперабельності та організаційних викликах цифровізації.

Таким чином, простежується закономірність: у вітчизняній науці пріоритет надається концептуально-правовим і термінологічним аспектам цифрової взаємодії, зарубіжні автори тяжіють до аналізу прикладних моделей, технологічних рішень та управлінських інновацій.

Праці цих та інших учених стали важливою методологічною основою дисертаційного дослідження, сприяли побудові логічних зв'язків між окремими змістовними блоками роботи, забезпечили достатній рівень інформаційного підґрунтя для розробки практичних рекомендацій для удосконалення механізмів

цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. Водночас, попри наявність значного масиву наукових розробок, безпосередньо чи опосередковано дотичних до проблематики дослідження, залишається потреба в оновленні теоретичних підходів і поглибленні наукових пошуків у цій сфері. Це зумовлює необхідність розробки нових науково обґрунтованих механізмів, які враховуватимуть сучасні виклики цифрової трансформації, інституційних змін та європейської інтеграції. Сукупність наведених аргументів і визначила актуальність обраної теми дисертації.

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

Дисертаційне дослідження виконане у межах науково-дослідної роботи, у Карпатському національному університеті імені Василя Стефаника за темою: «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (номер державної реєстрації 0120U100494). Внесок автора полягає в розробці пропозицій щодо пріоритетних напрямів удосконалення механізмів цифрової взаємодії органів публічної влади для ефективного розвитку електронного урядування.

*Метою* дослідження є теоретико-методологічне обґрунтування механізмів цифрової взаємодії органів публічної влади та розробка практичних рекомендацій щодо удосконалення їх функціонування в умовах розвитку електронного урядування.

Для досягнення зазначеної мети поставлено такі *завдання*:

- проаналізувати стан наукових досліджень проблем цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування;
- уточнити понятійно-категорійний апарат дослідження, визначити взаємозв'язок між суміжними термінами;
- з'ясувати стан та особливості механізмів цифрової взаємодії та інтегрованості інформаційних систем органів публічної влади в Україні та світі;
- проаналізувати безпекові виклики та можливості цифрової взаємодії

органів публічної влади в Україні;

– обґрунтувати практико-орієнтовані пропозиції щодо запровадження інтегрованості інформаційних систем органів публічної влади як чинника удосконалення механізмів цифрової взаємодії;

– розробити комплексну оцінювальну методику функціонування механізмів цифрової взаємодії органів публічної влади, яка підкреслить інтеграцію інструментів контролю, оцінки та організаційно-технічного забезпечення цифрових процесів;

– сформулювати комплекс рекомендацій щодо пріоритетних напрямів удосконалення механізмів цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування.

*Об'єкт дослідження* – система публічного управління в умовах електронного урядування.

*Предмет дослідження* – механізми цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування.

*Методи дослідження.* Методологічною основою дисертаційного дослідження є комплекс загальнонаукових та спеціально-наукових методів, які дозволили забезпечити всебічний, системний та об'єктивний аналіз механізмів цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. Використання зазначених методів забезпечило формування науково обґрунтованих висновків, рекомендацій та пропозицій, що обумовлюють формування наукової новизни дослідження. Зокрема: *індуктивний та дедуктивний метод* застосовано для окреслення та аналізу наукових розробок, дослідження ключових понять, зокрема: «органи публічної влади»; «механізми цифрової взаємодії органів публічної влади»; «електронне урядування»; з'ясування їх взаємозв'язку із суміжними термінами; *історичний метод* дав змогу дослідити генезу розвитку цифрової сумісності та взаємодії інформаційних систем органів публічної влади; *метод компаративного аналізу здобутих даних* уможливив визначення та порівняння ключових характеристик механізмів цифрової взаємодії та інтегрованості інформаційних систем органів

публічної влади у провідних країнах світу та Україні; *проблемно-науковий, прогностичний метод* дозволив обґрунтувати перспективні напрями удосконалення механізмів цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування; *метод моделювання* застосовано для вироблення пропозицій щодо шляхів удосконалення механізмів цифрової взаємодії органів публічної влади та розробки вітчизняної оціночної методики у досліджуваній сфері; *метод формалізації, узагальнення* використано для узагальнення опрацьованих матеріалів з метою формування висновків і рекомендацій за підсумками дослідження.

Сформульовані за результатами дослідження висновки та рекомендації створюють основу для впровадження інноваційного підходу до функціонування механізмів цифрової взаємодії органів публічної влади, зокрема через обґрунтування практико-орієнтованих пропозицій та формування комплексу рекомендацій щодо пріоритетних напрямів їх удосконалення в умовах розвитку електронного урядування. Результати дослідження можуть бути безпосередньо інтегровані в науково-практичні розробки органів державної влади та місцевого самоврядування, забезпечуючи підвищення ефективності міжвідомчої координації, сумісності інформаційних систем, кіберстійкості державних сервісів та формування прозорого, підзвітного і інклюзивного електронного урядування в Україні.

*Наукова новизна одержаних результатів* полягає в тому, що в процесі дисертаційного дослідження вирішено важливе науково-практичне завдання публічного управління – здійснено теоретико-методологічне обґрунтування механізмів цифрової взаємодії органів публічної влади та розроблено на цій основі практичні рекомендації щодо удосконалення їх функціонування в умовах розвитку електронного урядування. Виходячи з цього у дисертації, зокрема:

*уперше:*

– розроблено архітектурну модель механізмів цифрової взаємодії органів публічної влади, яка базується на принципах інтероперабельності інформаційних систем і містить такі компоненти: *цільово-функціональний*

*механізм (організаційна архітектура)*, що визначає управлінські функції органів влади, типові адміністративні процеси (реєстрація, надання послуг, видача дозволів), а також стратегічні орієнтири цифрової трансформації, зокрема прозорість і підзвітність; *інформаційно-комунікативний механізм (інформаційна архітектура)*, який регламентує стандартизацію та обіг даних між органами влади, забезпечуючи сумісність на основі стандартів і платформ типу «Трембіта» та національного порталу відкритих даних; *сервісно-інтеграційний механізм (прикладна архітектура)*, що реалізує управлінські функції через цифрові сервіси, відкриті API, реєстрові шлюзи і системи електронного документообігу; *інфраструктурно-технологічний механізм (технічна архітектура)*, який забезпечує технічні умови сумісності, безпеки й безперервності роботи інформаційних систем, включно з серверними платформами, хмарною/туманною інфраструктурою і засобами кіберзахисту; *кадрово-ресурсний механізм (архітектура людського потенціалу)*, що охоплює систему кадрової підготовки, розвитку цифрових компетенцій та формування відповідної культури у органах публічної влади. Модель інтегрує п'ять типів інтеоперабельності: технічну, семантичну, організаційну, юридичну і політичну, сприяючи формуванню цілісного, масштабованого і безпечного інформаційного простору для ефективної цифрової взаємодії органів публічної влади на різних рівнях управління та формуючи системний фундамент для сталого розвитку електронного урядування в Україні;

– обґрунтовано застосування комплексної оцінювальної методики у вигляді матриці моніторингу функціонування механізмів цифрової взаємодії органів публічної влади, яка *інтегрує контрольні, оцінні та організаційно-технічні інструменти*, забезпечуючи системне вимірювання *технічних* (кількість інтегрованих систем, частота збоїв, наявність API); *семантичних* (відповідність даних міжнародним стандартам); *організаційних* (рівень цифрових компетенцій персоналу, наявність політик цифрового управління); *правових* (ступінь імплементації директив ЄС, внутрішні регламенти цифрової взаємодії); *кадрово-ресурсних* (навчання та підготовка працівників),

кібербезпекових (сертифікація відповідності ISO/IEC 27001, частота інцидентів); *соціальних* (рівень задоволеності користувачів, доступність сервісів для вразливих груп) та *ефективнісних* (середній час обробки запитів, кількість наданих електронних послуг) параметрів; поєднуючи різнотипні шкали вимірювання (кількісні, бінарні, якісні, агреговані індекси) і мультиджерельну систему збору даних (державні реєстри, системні логи, внутрішні звіти, нормативні акти, аналітика фронт-офісів, опитування користувачів), що дозволяє отримувати репрезентативні та валідні оцінки, одночасно враховувати об'єктивні технічні метрики, суб'єктивні якісні оцінки; інтегрувати результати SWOT-аналізу для виявлення внутрішніх можливостей та зовнішніх ризиків, тим самим формуючи цілісну основу для evidence-based policy (політики, заснованої на доказах) у сфері електронного урядування, спрямовану на стратегічне планування, підвищення цифрової зрілості органів публічної влади та забезпечення прозорості, підзвітності й стійкості цифрових трансформацій;

*удосконалено:*

– структурно-функціональний підхід до аналізу інформаційних систем (ІС) у публічному управлінні, який враховує: *технологічну складову ІС* – поєднання апаратного, програмного, телекомунікаційного забезпечення, баз даних, аналітичних модулів, а також систем управління знаннями; *типологію ІС* за функціональним призначенням: системи обробки транзакцій (TPS), інформаційні системи управління (MIS), системи підтримки прийняття рішень (DSS), інформаційні системи для керівників (ESS); *соціальну та комунікативну функцію* – здатність ІС забезпечувати двосторонню взаємодію між державою і громадянами, сприяти прозорості, підзвітності, зворотному зв'язку, що є основою цифрової довіри у взаємодії «влада – громадянське суспільство»;

– періодизацію історичних етапів розвитку інформаційних систем ХХІ століття у контексті переходу від інформаційного до цифрового суспільства, що охоплює такі ключові фази: розширення базового доступу до інтернету та комп'ютерів (1998-2000); поширення інформаційно-комунікативних технологій та створення національних урядових порталів (2000-2005); розбудову

інфраструктури широкосмугового зв'язку (2010-2015); впровадження концепції «Уряд як платформа» і політики відкритих даних (2015-2020); стрімкий розвиток цифрових сервісів у період пандемії COVID-19 та після неї (2020-2025); прийняття національних планів цифрового розвитку та акцент на технологіях Індустрії 4.0 і цифрових навичках суспільства (2025-2030);

*набули подальшого розвитку:*

– підходи до формування концепції цифрової інклюзії та участі громадян, яка тлумачить цифрові технології не лише як інструмент, але як *середовище партисипативного управління*, що формує нові виміри публічної комунікації та соціальної відповідальності влади, які полягають у: *розширенні доступу до публічних послуг та інформації* через електронні платформи, мобільні додатки, відкриті дані; *створенні багатоканального середовища цифрової участі* (застосування соціальних мереж, порталів електронної демократії, механізмів електронних петицій, бюджетів участі); *формуванні горизонтальних зв'язків у громадянському суспільстві* завдяки платформам для співучасті, колективного моніторингу, краудсорсингу; *інституціоналізації цифрової відкритості та підзвітності* (включення цифрових звітів, дашбордів та індикаторів ефективності діяльності органів публічної влади);

– узагальнення наукового доробку щодо тлумачення поняття «цифрова взаємодія органів публічної влади», серед яких виокремлено: *технологічний підхід*: цифрова взаємодія як автоматизований обмін даними між інформаційними системами (інтероперабельність); *інфраструктурно-функціональний підхід*: цифрове середовище для реального часу комунікації з інтеграцією сервісів (електронні платформи, хмарні рішення); *економічний підхід*: взаємодія як чинник підвищення ефективності управління за умов мінімальних транзакційних витрат; *соціально-комунікативний підхід*: цифрова взаємодія як форма залучення громадян до прийняття рішень через ІКТ; *правоорганізаційний підхід*: акцент на необхідності законодавчого закріплення форм і механізмів такої взаємодії;

– вихідні положення щодо відстеження кіберзагроз у системі цифрової

взаємодії органів публічної влади, що поєднують інституційно-функціональний та ризикологічний підходи до оцінювання кіберстійкості, операціоналізують процес відстеження через класифікацію загроз за джерелами та рівнями прояву, виокремлюють індикатори вразливості, визначають порогові значення ризику з алгоритмами реагування та раннього виявлення, а також передбачають застосування прогностичної аналітики на базі інструментів штучного інтелекту.

*Практичне значення одержаних результатів* полягає в тому, що положення й висновки, викладені в дисертації, формують методологічну й прикладну основу для вдосконалення механізмів цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. Сформульовані у роботі пропозиції можуть бути використані у процесі:

- розробки та удосконалення стратегічних і нормативно-правових актів щодо цифрової трансформації публічного управління, зокрема в частині інтероперабельності інформаційних систем;
- впровадження сучасних моделей цифрової взаємодії органів публічної влади;
- оптимізації організаційно-функціональної структури органів публічної влади з урахуванням вимог електронного урядування;
- підготовки, перепідготовки та підвищення кваліфікації публічних службовців у сфері цифрової трансформації та управління інформаційними системами.

Основні теоретичні положення дисертаційного дослідження та запропоновані висновки можуть бути використані:

- у практичній діяльності органів публічної влади (зокрема – у практичній діяльності органів публічної влади (центральної влади, органів місцевого самоврядування) для впровадження механізмів інтероперабельності та цифрової взаємодії;
- у подальших наукових дослідженнях, спрямованих на розробку сучасних концепцій цифрової трансформації публічного управління;
- у навчальному процесі при підготовці навчальних програм,

підручників і методичних матеріалів зі спеціальності 281 «Публічне управління та адміністрування».

Матеріали та результати дисертаційного дослідження впроваджено в роботі:

Дмитрівської громади Ніжинського району Чернігівської області при підготовці Плану заходів Дмитрівської селищної ради на 2025-2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року. Зокрема, пропозиції щодо цифрової рівності та інклюзії були враховані при формуванні заходів щодо забезпечення доступності та адаптації електронних послуг громади (веб-сайту, електронних реєстрів) до міжнародних вимог стандартів безбар'єрності (WCAG 2.1 - Настанови із забезпечення доступності веб-контенту, версія 2.1.), що дозволяє забезпечити рівний доступ до інформації і сервісів для всіх мешканців, включаючи маломобільні групи населення та осіб з порушеннями зору (довідка № 03/17 від 22.09.2025 р.);

Городоцької міської територіальної громади Хмельницького району Хмельницької області, зокрема, практичні пропозиції щодо посилення цифрової компетентності посадових осіб місцевого самоврядування (зокрема тих, хто працює із соціально вразливими сім'ями) були враховані у плануванні тренінгів для підвищення їхніх цифрових навичок та вміння працювати з інтегрованими інформаційними системами для обміну даними, а також використані при розробці внутрішнього Регламенту роботи з державними реєстрами при наданні адміністративних послуг (довідка № 38 від 10.10.2025 р.);

Хмельницької обласної ради при підготовці Стратегії регіонального розвитку Хмельницької області на 2021-2027 роки (оновлена редакція, затверджена рішенням обласної ради №13-26/2025 від 18 червня 2025 року). Зокрема, пропозиції щодо запровадження програм розвитку цифрового лідерства та підвищення кваліфікації публічних службовців були враховані при формуванні завдань Стратегії щодо посилення інституційної стійкості та кадрової спроможності обласних та місцевих органів влади; пропозиції щодо

запровадження механізмів проактивного врядування, орієнтованого на життєві події громадян, враховано при обґрунтуванні необхідності підвищення аналітичної спроможності обласної ради для прийняття управлінських рішень на основі оперативних цифрових даних. (довідка №2080/01-11 від 18.12.2025 р.).

*Особистий внесок здобувача.* Дисертаційне дослідження є самостійною науковою працею. Усі основні ідеї, концептуальні підходи, положення та висновки, що становлять наукову новизну й практичне значення, належать авторові та виконані ним особисто.

*Апробація результатів дослідження* здійснювалася у доповідях та повідомленнях на наукових конференціях: «Science And Innovation Of Modern World» (Лондон, Велика Британія, 28–30 вересня 2022 р.); «Science And Technology: Problems, Prospects And Innovations» (Осака, Японія, 19-21 жовтня 2022 р.); «Priority Directions of Science Development» (Гамбург, Німеччина, 6-8 лютого 2023 р.); «Scientific Progress: Innovations, Achievements and Prospects» (Мюнхен, Німеччина, 3-4 квітня 2023 р.); «Education and Science of Today: Intersectoral Issues and Development of Sciences» (Кембридж, Велика Британія, 18 серпня 2023 р.); «Science and Society: Modern Trends in a Changing World» (Відень, Австрія, 5-7 серпня 2024 р.); «Scientific Achievements of Contemporary Society» (Лондон, Велика Британія, 15-17 серпня 2024 р.).

*Публікації.* Загальні положення та зміст дисертації відображено у 12 публікаціях, зокрема в 4 статтях у наукових фахових виданнях з публічного управління, 1 – у міжнародному виданні, семи тезах доповідей у матеріалах міжнародних науково-практичних конференцій.

*Структура дисертації.* Дисертація складається зі вступу та трьох розділів, поділених на підрозділи. Дослідження завершується загальними висновками. Робота містить 11 таблиць, 8 рисунків. Загальний обсяг дисертації становить 231 сторінка, з них 186 сторінок основного тексту. Список використаних джерел налічує 218 найменувань, значна частина з яких іноземною мовою.

## **РОЗДІЛ 1. ТЕОРЕТИКО-ІСТОРИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМ ЦИФРОВОЇ ВЗАЄМОДІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ**

### **1.1 Аналіз ключових понять дослідження, їх взаємозв'язок із суміжними термінами**

Початковим етапом будь-якого наукового дослідження є формулювання понятійно-категоріального апарату, який становить інструмент для осмислення сутності досліджуваного явища. Саме через уточнення дефініцій ключових понять стає можливим окреслення меж предмета дослідження, встановлення його внутрішньої логіки та взаємозв'язків з іншими науковими категоріями. Як слушно зауважує Я. Радиш, обґрунтування й формування наукових дефініцій - це одна з найбільш складних і водночас визначальних процедур у структурі наукового пізнання [1, с. 197].

Ця думка поділяється багатьма вченими всього світу. У цьому контексті узгодження понять «механізми цифрової взаємодії», «органи публічної влади», «електронне урядування», а також суміжних термінів, що відображають сучасні трансформаційні процеси в системі публічного управління, дозволяє сформулювати цілісне бачення предметного поля дослідження.

Комунікація між владою та суспільством упродовж історії формувалась під впливом конкретно-історичних умов і технологічних можливостей кожного етапу розвитку. У сучасну епоху цифровізації вона набула якісно нового змісту: цифрові технології докорінно змінили архітектуру взаємодії між державою та громадянами, усунувши чимало традиційних комунікативних бар'єрів. З'явилися нові моделі публічного управління - електронний уряд, держава у смартфоні, розумна держава, які відображають перехід до нової управлінської парадигми.

Трансформація комунікативних механізмів супроводжується і зміною логіки політико-управлінських процесів, у яких центральне місце займає

громадянин як активний учасник прийняття рішень. Цей процес відбувається в умовах посилення ролі інформаційно-комунікативних технологій, що виступають каталізаторами змін у публічному секторі. Водночас, попри понад 60-річну історію використання інформаційно-комунікативних технологій у публічному управлінні, проблематика ефективної цифрової взаємодії між владою та громадянами залишається відкритою.

Інноваційне застосування цифрових технологій передбачає не лише технічне оновлення, але й глибоку інституційну трансформацію управлінських процесів. Саме тому вивчення ключових понять і категорій, які відображають цю трансформацію, є необхідною передумовою для подальшого аналізу механізмів цифрової взаємодії в умовах розвитку електронного урядування.

Проблема комунікації влади і суспільства є своєрідною і вирішувалася відповідно до конкретно-історичних умов розвитку суспільства на основі двох аспектів – політико-філософського бачення необхідності такої комунікації та комунікативних можливостей суспільства (інструментів комунікативної взаємодії), які технологічно відповідали рівню розвитку суспільних відносин, матеріальної та нематеріальної культури, характеру політичного устрою тощо.

У процесі переходу до цифрового суспільства технологічні передумови комунікації зазнали суттєвої трансформації: сучасні цифрові рішення значною мірою нівелювали бар'єри взаємодії, що раніше були обумовлені обмеженнями технічного розвитку. Свідченням цього є поява та поширення новітніх підходів у сфері публічного управління — електронного урядування, концепцій «розумної держави» та «держави у смартфоні», які відображають технологічну основу сучасного етапу еволюції публічно-управлінських процесів.

Логіка суспільних трансформацій в епоху цифрового суспільства визначається поступовим рухом до розвинутих форм сучасної демократії, які передбачають широке залучення громадян до процесу прийняття рішень. Незважаючи на 60 років використання, проблеми, пов'язані з інформаційно-комунікативними технологіями в публічному управлінні, все ще існують. Дослідження свідчать про безпосередній пропорційний зв'язок між доступом до

Інтернету та частотою його використання, а також між використанням Інтернету та схильністю до використання послуг приватного сектору, таких як інтернет-банкінг. Разом з тим, це зовсім не означає автоматичного переходу до запровадження електронних адміністративних послуг у публічному управлінні. Оскільки уряди стикаються зі складними викликами, очікується, що вони будуть інноваційно підходити до використання ресурсів та організації надання послуг. Інформаційно-комунікативні та цифрові технології розглядаються як фактор трансформаційних змін для вирішення завдань розбудови електронного урядування шляхом підвищення ефективності, результативності, прозорості, підзвітності та/або інклюзивності.

Термін «електронне врядування» був вперше запропонований у 1993 році в Національному огляді ефективності США, в той час як термін «електронний уряд» набув поширення приблизно в 1997 році. Тим не менш, ІКТ відіграють важливу роль у наданні послуг у державному секторі з середини ХХ століття [2, с. 112].

Електронне урядування розглядається як шлях до досягнення належного управління за допомогою інформаційно-комунікативних та цифрових технологій шляхом підвищення ефективності урядових операцій, зміцнення демократії, підвищення прозорості та підзвітності, а також надання кращих послуг громадянам і бізнесу. Електронне урядування об'єднує людей, процеси, інформацію та технології для покращення надання адміністративних послуг, доступу до інформації та публічного управління в цілому.

Електронний уряд стає значною частиною поточних реформ та трансформації, що дозволяє підвищити ефективність та результативність роботи. Дослідники розглядають цю трансформацію як інструмент формування та розвитку партисипативного управління, яке більш орієнтоване на громадян та максимально використовує новітні технології у цьому процесі [3].

Питання тлумачення поняття «електронне урядування» активно досліджується на міжнародному рівні, про що свідчать численні аналітичні, нормативні та наукові джерела. Серед них ключову роль відіграють документи

Організації Об'єднаних Націй (ООН), Організації економічного співробітництва та розвитку (ОЕСР), Організації американських держав (ОАС), а також публікації провідних академічних платформ, зокрема IGI Global.

Так, у Щорічному дослідженні електронного уряду ООН (UNDESA, 2014) [4] увага акцентується на концептуальній основі електронного уряду як інструменту майбутнього, що формує нові підходи до урядування через цифрові сервіси. У документі аналізується еволюція надання державних послуг за допомогою ІКТ, рівень доступності та ступінь інтеграції цифрових сервісів у функціонування органів влади. Основний наголос зроблено на моделі «government supply», тобто ініціативі держави у впровадженні ІКТ.

Глосарій ОЕСР (2022) подає визначення електронного уряду з акцентом на використанні інноваційних інформаційно-комунікативних технологій для виконання всього спектра державних функцій [5]. ОЕСР тлумачить е-уряд як потенційно трансформаційне явище, здатне змінити структуру, функціонал і якість діяльності органів публічного управління. Згідно з цим підходом, важливим є не лише впровадження ІКТ, а й глибина їх інтеграції в інституційне середовище.

Організація американських держав (ОАС) у своїх аналітичних документах [6] розглядає е-уряд у площині ефективності, прозорості й залучення громадян. Основна увага приділена функціональному призначенню ІКТ як засобу демократизації урядових процесів, підвищення якості послуг і формування механізмів громадської участі в управлінні.

Академічна платформа IGI Global пропонує узагальнене, комплексне трактування поняття, яке охоплює як технологічний, так і управлінський, комунікативний та сервісний виміри. Автори ресурсів IGI Global розглядають електронний уряд як багатовимірне явище, що реалізується через взаємодію уряду з громадянами (G2C), бізнесом (G2B), іншими органами влади (G2G) і працівниками (G2E). Водночас, підкреслюється роль ІТ як платформи для інформаційного обміну, електронних транзакцій і створення цифрового середовища для реалізації публічної політики [7].

Світовий банк, зокрема, визначає електронний уряд як застосування інформаційних та цифрових технологій для трансформації взаємодії влади з громадянами, бізнесом та іншими органами публічної влади, наголошуючи, що електронний уряд є новим способом надання якісних державних послуг [8].

Таким чином, у науковій літературі простежується умовний поділ підходів до визначення електронного уряду за ознакою орієнтації – або на ініціативи з боку держави («supply-driven» модель), або на запити та участь громадськості («demand-driven» модель). Зведені характеристики основних підходів подано у табл. 1.1.

Таблиця 1.1

## Підходи до визначення поняття «електронне урядування»

Автор	Зміст визначення
UNDESA [4]	«Електронне урядування» – використання ІКТ та їх застосування урядом для надання інформації та державних послуг населенню
Глосарій статистичних термінів Організації з економічного співробітництва та розвитку (ОЕСР) [5]	Термін «електронний уряд» зосереджується на використанні урядами нових інформаційно-комунікативних технологій (ІКТ) у застосуванні до всього спектру державних функцій. Зокрема, мережевий потенціал, пропонований Інтернетом і пов'язаними з ним технологіями, має потенціал для трансформації структур і роботи уряду.
Organization of American States [6]	Електронний уряд (або е-уряд) – це застосування інформаційно-комунікативних технологій (ІКТ) до урядових функцій та процедур з метою підвищення ефективності, прозорості та участі громадян.
Платформа IGI Global [7]	Електронний уряд (від англ. electronic government, також відомий як e-gov, цифровий уряд, онлайн-уряд або в певному контексті трансформаційний уряд) – це використання інтернет-технологій як платформи для обміну інформацією, надання послуг та здійснення транзакцій з громадянами, бізнесом та іншими гілками влади.

## Продовження таблиці 1.1

	Електронний уряд може застосовуватися законодавчою, судовою або адміністративною владою з метою підвищення внутрішньої ефективності, надання державних послуг або процесів демократичного врядування.
	Електронний уряд – це електронне надання урядової інформації та послуг 24 години на добу, сім днів на тиждень
	Електронний уряд – це застосування ІТ до урядових послуг та процедур для надання державних послуг та інформації громадянам, бізнесу та урядам в електронному вигляді
	Надання державних послуг в режимі онлайн, що дає можливість розширити доступ громадян до влади, зменшити урядову бюрократію, розширити участь громадян у демократії та підвищити оперативність реагування органів влади на потреби громадян.
	Електронний уряд (е-уряд) – це використання інформаційних технологій для надання державних послуг в режимі онлайн, що має на меті забезпечення більш швидкого та якісного обслуговування зацікавлених сторін. Його можна розділити на чотири основні категорії, а саме: «Уряд-громадянин» (G2C), «Уряд-бізнес» (G2B), «Уряд-уряд» (G2G) та «Уряд-працівник» (G2E).

Джерело: узагальнено автором за [4-8]

Таким чином, приходимо до висновку, що електронний уряд визначається через поняття багатовимірності.

Визначення адміністративних, електронних та державних послуг тісно пов'язані з темою дослідження, оскільки вони є ключовими компонентами механізмів цифрової взаємодії органів публічної влади.

Відповідно до статті 1 Закону України «Про адміністративні послуги», адміністративна послуга визначається як результат реалізації владних повноважень суб'єктом її надання за зверненням фізичної чи юридичної особи, спрямований на набуття, зміну або припинення прав та/або виконання обов'язків відповідно до законодавства [9]. Таким чином, адміністративні послуги – це дії

органів державної влади та місцевого самоврядування, орієнтовані на забезпечення реалізації правового статусу заявників у межах установлених норм. До них належать, зокрема, оформлення дозволів, ліцензій і сертифікатів, проведення державної реєстрації актів цивільного стану, майнових прав, транспортних засобів та інших юридично значущих процедур. Вітчизняна правова база передбачає, що їх надання ґрунтується на принципах законності, доступності, відкритості, прозорості, оперативності та належної якості.

Електронні послуги (е-послуги) – це різновид адміністративних послуг, що реалізуються із застосуванням інформаційно-комунікаційних і цифрових технологій, насамперед через мережу Інтернет. Вони функціонують як цифрова форма традиційних адміністративних процедур, забезпечуючи можливість дистанційної взаємодії громадян і суб'єктів господарювання з органами публічної влади та сприяючи оперативному й зручному доступу до необхідних сервісів [10].

Електронні послуги є складовою частиною концепції електронного урядування, яке спрямоване на підвищення ефективності, прозорості та доступності публічного управління. Впровадження електронних послуг зменшує адміністративні бар'єри, скорочує час на обробку запитів та знижує корупційні ризики. Також у законодавстві зазначено, що електронні послуги можуть бути як адміністративними, так і іншими, наприклад, соціальними чи інформаційними, і надаються автоматизовано, часто без втручання людини

У науковій та нормативній літературі англійський термін «public services» традиційно перекладається як «публічні послуги», проте в українському дискурсі довгий час побутував синонімічний термін «державні послуги», що зумовлено впливом усталених підходів до перекладу терміна «public administration» як «державне управління» або «публічна адміністрація». Відтак, у Концепції адміністративної реформи в Україні паралельно використовувались такі терміни, як державні, публічні та управлінські послуги, при цьому чітке розмежування між ними фактично не проводилось [11].

У сучасному розумінні державні (публічні) послуги охоплюють широкий

спектр сервісів, які надаються органами публічної влади, їхніми структурами та підпорядкованими установами громадянам, підприємствам та іншим суб'єктам. До цієї категорії належать не лише адміністративні послуги, а й соціальні, освітні, медичні, культурні та інші види сервісів. Основними критеріями якості таких послуг виступають доступність, своєчасність, результативність, законність і задоволеність споживачів, що відповідає сучасним стандартам публічного управління.

Вважаємо, що розуміння адміністративних, електронних та державних послуг у зазначеному контексті є необхідним для досягнення мети дослідження. Це дозволяє комплексно підходити до аналізу механізмів цифрової взаємодії органів публічної влади, враховуючи всі аспекти, які впливають на ефективність, прозорість та доступність державних послуг в умовах розвитку електронного урядування.

Комунікація в умовах цифрових суспільних трансформацій є одним з найважливіших інструментів публічного управління з огляду на технологізацію суспільства та соціальних зв'язків всередині нього. Особливо важливим для нас є розгляд сутності цього процесу у контексті взаємодії «публічна влада – громадянське суспільство».

Аналіз взаємодії інститутів громадянського суспільства з органами публічної влади крізь призму правових і управлінських засад дає підстави розглядати громадянське суспільство як саморегульований соціальний механізм, що виконує як трансформаційну, так і стримувальну функції у протидії авторитарним тенденціям. Інструментальним підґрунтям реалізації цих функцій виступають інститути місцевого самоврядування, волонтерські, благодійні та добровольчі ініціативи, ефективність яких підтверджується сучасним досвідом державотворчих процесів в Україні. У зв'язку з цим актуалізується потреба формування дієвих механізмів інтеграції комунікативних практик влади та суспільства, де ключову роль відіграють цифрові технології як інструмент підвищення ефективності взаємодії та координації.

Сучасний цифровий світ обертається навколо формування, обміну та

використання інформації у електронній формі, дані накопичуються, структуруються, зберігаються та об'єднуються в мережі, створюючи глибоке відчуття соціальної пов'язаності та глобальної спільноти. Скорочуючи витрати на інформацію, цифрові технології скасовують бар'єри для комунікації громадян, підприємств та органів публічної влади. Технічно вони забезпечують процес створення усіх видів інформації, включаючи аудіо- та відеосигнали, та переведення їх у цифровий формат, який обробляється електронними пристроями.

Відомо, що реалізація цифрової взаємодії органів публічної влади здійснюється *через застосування інформаційних систем*, що в контексті даного дослідження актуалізує потребу аналізу відповідних термінів і понять.

Л. Віттакер (Louise Whittaker) визначає інформаційні системи як мережі, призначені для загального використання в певній галузі чи організації. Дослідниця виокремлює три покоління інформаційних систем органів публічної влади:

1. системи упаковки інформації, які забезпечують мінімальний обмін;
2. системи пошуку інформації та обміну даними, але не процесами;
3. системи обробки інформації, які забезпечити максимальний обмін даними та процесами [12].

Як зазначає Ючонг Лі (Yuchong Li), інформація та знання стали життєво важливими економічними ресурсами. Однак, поряд із новими можливостями, розвиток інформаційних систем несе й нові загрози, які стосуються безпеки зберігання баз даних та несанкціонованого доступу до них. Цифровий простір поставив перед урядами нові завдання безпеки. Низька вартість входу, анонімність, подекуди слабка визначеність географічного району та відсутність публічної прозорості у кіберпросторі призвели до того, що в ньому з'явилися сильні та слабкі учасники, включаючи інформаційні системи органів публічної влади, комерційні бази даних, організовані групи та навіть окремі особи [13].

Китайські дослідники Лей Чжан та Юнген Гу (Lei Zhang, Yonggen Gu) до основних компонентів інформаційних систем відносять комп'ютерне

обладнання та програмне забезпечення, телекомунікації, бази даних та сховища даних, людські ресурси та процедури [14].

Апаратне забезпечення, програмне забезпечення, дані та телекомунікації складають цифрові технології, які на сучасному етапі міцно увійшли до функціонування органів публічної влади. Основні компоненти інформаційних систем наведені на рис. 1.1.



Рис 1.1. Основні компоненти інформаційних систем

Джерело: узагальнено автором на основі [10]

*Апаратне забезпечення* становить матеріальну основу цифрових технологій і охоплює фізичні пристрої: комп'ютери, накопичувачі даних, периферійні засоби введення та виведення інформації, планшети та інші технічні інструменти. Сучасні тенденції розвитку характеризуються поступовим здешевленням обладнання на тлі зростання його продуктивності та обсягів пам'яті. Водночас екологічні наслідки виробництва й використання технічних засобів викликають зростаюче занепокоєння. Паралельно поширюються хмарні технології, що забезпечують віддалене зберігання даних і доступ до них через телекомунікаційні мережі.

*Програмне забезпечення* поділяється на системне та прикладне. Системне програмне забезпечення, зокрема операційні системи, забезпечує функціонування апаратних ресурсів, керує файлами та процесами і створює користувацьке середовище взаємодії з комп'ютером. Прикладне програмне забезпечення орієнтоване на виконання конкретних користувацьких завдань і реалізацію спеціалізованих функцій. Отже, системне програмне забезпечення формує базові умови використання технічних ресурсів, тоді як прикладне – забезпечує практичне виконання визначених операцій.

*Дані* – це стратегічний ресурс у вигляді систематизованих фактів, який слугує об'єктивною базою для прийняття обґрунтованих рішень і мінімізації ризиків. Завдяки їх аналізу можна оцінити реальну ефективність процесів, виявити приховані закономірності та оптимізувати подальшу діяльність для досягнення максимальних результатів.

*Телекомунікації* забезпечують підключення комп'ютерних систем і різноманітних пристроїв з метою передавання та обміну інформацією. Побудова мереж можлива як у дротовому, так і в бездротовому форматі: до дротових належать, зокрема, оптоволоконні та коаксіальні кабелі, тоді як бездротові рішення базуються на використанні радіо- та мікрохвильових технологій [14, с. 108].

М. Мартін (Matthew Martin) виокремлює кілька ключових типів інформаційних систем. Першу групу становлять системи підтримки операцій,

орієнтовані на забезпечення виконання стандартних процедур, передусім у фінансовій сфері. Прикладом є системи обробки транзакцій, що широко застосовуються в банківському секторі та дають змогу оцінювати ефективність бізнес-процесів і якість надання послуг [15].

*Інформаційні системи управління* становлять окрему категорію інформаційних систем і являють собою інтегровані комплекси апаратних та програмних засобів, що забезпечують виконання ключових функцій установи. Вони сприяють збору даних із різних цифрових джерел та онлайн-платформ, після чого отримана інформація піддається аналітичній обробці з метою моніторингу й контролю управлінських процесів, а не обов'язково довгострокового зберігання.

*Системи підтримки ухвалення рішень* орієнтовані на забезпечення обґрунтованості управлінських дій шляхом аналізу складної та динамічної інформації, що характеризується високим рівнем невизначеності та мінливості. Такі системи можуть функціонувати як у повністю автоматизованому режимі, так і за участю людини, однак найвищу ефективність демонструє їх поєднання, коли аналітичні можливості комп'ютерних технологій доповнюються експертним оцінюванням користувачів.

*Інформаційні системи керівників* є системами підтримки управління та прийняття рішень на рівні першої особи [15]. У сучасній науковій та прикладній літературі простежується розмаїття підходів до визначення цього поняття. Джерела [16-21] представляють авторитетні енциклопедичні, академічні та технічні джерела, в яких термін «інформаційна система» розкривається крізь призму її структурних компонентів (програмне забезпечення, апаратне забезпечення, телекомунікативна інфраструктура), функціонального призначення (збір, обробка, зберігання, аналіз, передача інформації), а також соціального та управлінського контексту (використання у державному управлінні, бізнесі, аналітиці даних тощо).

Усі ці підходи акцентують увагу на інтегративній природі інформаційної системи як сукупності взаємопов'язаних технологічних та організаційних

компонентів, що забезпечують ефективне управління інформаційними потоками. Основні трактування поняття «інформаційні системи» узагальнено у табл. 1.2.

Таблиця 1.2

## Підходи до визначення поняття «інформаційні системи»

Автор	Зміст визначення
Britannica [13]	Інтегрований набір компонентів для збору, зберігання та обробки даних, а також для надання інформації, знань та цифрових продуктів
Emeritus [14]	Це поєднання програмного забезпечення, обладнання та телекомунікативних мереж для збору корисних даних, особливо в організації
Master's in Data Science [15]	Це мережа, що використовується для збирання, зберігання, обробки, аналізу та розповсюдження даних
Collat school of business [16]	Це узагальнене поняття, що охоплює сукупність мережевих, апаратних і програмних компонентів, які використовуються користувачами та організаціями для опрацювання й осмислення даних та їх подальшого застосування. Окрім інтерпретації інформації, такі системи забезпечують її збирання, оброблення, зберігання та поширення з метою підтримки діяльності й ухвалення рішень.
Information Technology Laboratory [17]	Дискретна сукупність інформаційних ресурсів, організована для збирання, оброблення, зберігання, використання, поповнення, поширення та знищення інформації
Technopedia [18]	Інформаційна система (ІС) – це сукупність декількох одиниць обладнання, що беруть участь у зборі, обробці, зберіганні та поширенні інформації

Джерело: узагальнено автором на основі [16-21].

Інформаційно-комунікативні технології сприяють інноваціям і, знижуючи транзакційні витрати майже до нуля, підвищують ефективність, оскільки існуючі види діяльності і послуги стають дешевшими, швидшими або зручнішими. Вони мають потенціал для збільшення інклюзивності, оскільки громадяни отримують

доступ до послуг, які раніше були поза їхньою досяжністю. ІКТ відіграють вирішальну роль у досягненні цілей розвитку з огляду на покращення комунікації, обмін знаннями та інформацією, необхідними для суспільних процесів. Стаючи ключовим фактором, що сприяє удосконаленню публічного управління, вони здатні впливати на увесь спектр людської діяльності. ІКТ є потужними, якщо не необхідними, інструментами для розширення заходів з розвитку і досягнення результатів діяльності [22]. Цифрові технології також здійснюють значний внесок у прискорення потоку інформації та знань між урядом і громадянами та трансформації їхніх відносин. Такі терміни, як Government 2.0 стали популярними, характеризуючи спільний характер управління, отриманого від участі через ІКТ. Відповідно до Програми розвитку ООН, перед усіма країнами стоїть завдання створення та впровадження системи належного врядування, яка сприяє та підтримує людський розвиток.

Повертаючись до аналізу термінів і понять, слід зауважити, що визначення цифрової взаємодії формується науковцями, базуючись на різних підходах. Одні науковці тлумачать цифрову взаємодію як автоматизований обмін даними між інформаційними базами даних, додатками, іншими комп'ютерними системами та утворюють ключовий компонент в усіх мережевих комп'ютеризованих системах [23; 24].

Інші розуміють це поняття як цифрове середовище, у якому спеціальний програмно-апаратний комплекс забезпечує прямий взаємозв'язок у реальному часі та має набір відповідних функцій і сервісів задля комунікації між споживачами та надавачами (виробниками) товарів чи послуг [25; 26].

Треті визначають поняття цифрової взаємодії через призму економічних характеристик, акцентуючи увагу на можливості досягнення високого рівня ефективності функціонування органів публічної влади у економічній сфері за найменших затрат [27; 28].

Таким чином, визначення поняття цифрової взаємодії пов'язується із конкретним аспектом або сферою публічного управління. Підходи до визначення поняття «цифрова взаємодія» згруповані у табл. 1.3.

Метою інформаційної системи є надання певної послуги або процесу за участю широкої громадськості. На відміну від цього, непублічна або приватна інформаційна система надає послуги, тісно пов'язані з певною організацією, виконання певних завдань, які часто є внутрішніми адміністративними процесами.

Таблиця 1.3

## Підходи до визначення поняття «цифрова взаємодія»

Автор	Зміст визначення
Stephen O'Connor [23]; Ramya Mohanakrishnan [24]	Це автоматизований обмін даними між інформаційними базами даних, додатками, іншими комп'ютерними системами та утворюють ключовий компонент в усіх мережевих комп'ютеризованих системах
О. Баранов [25]; Michael E. Porter, Victor E. Millar [26]	Це цифрове середовище, в якому спеціальний програмно-апаратний комплекс забезпечує прямий взаємозв'язок у реальному часі та має набір відповідних функцій і сервісів задля комунікації між споживачами та надавачами (виробниками) товарів чи послуг
Т. Олешко, Н. Касьянова Н, С. Смерічевський [27]; Deanira Laze [28]	Поняття цифрової взаємодії тлумачиться через призму економічних характеристик, акцентуючи увагу на можливості досягнення високого рівня ефективності управління за найменших затрат

Джерело: узагальнено автором за [23-28]

Суб'єкти інформаційно-цифрового простору, зазвичай належать до наступних категорій (рис.1.2):

*C (Customers)*: приватні особи та домашні господарства/сім'ї в ролі громадян як споживачів послуг, клієнтів;

*B (Business)*: комерційні компанії та інші некомерційні організації;

*G (Governments)*: суб'єкти публічного управління - органи державної влади, органи місцевого самоврядування; державні установи та інституції на різних рівнях управління (центральний, регіональний, місцевий).

При цьому варто зазначити, що термін «цифрова взаємодія органів публічної влади» поки що не знайшов узгодженого наукового тлумачення у науковому дискурсі, продовжує досліджуватись та потребує законодавчого закріплення.

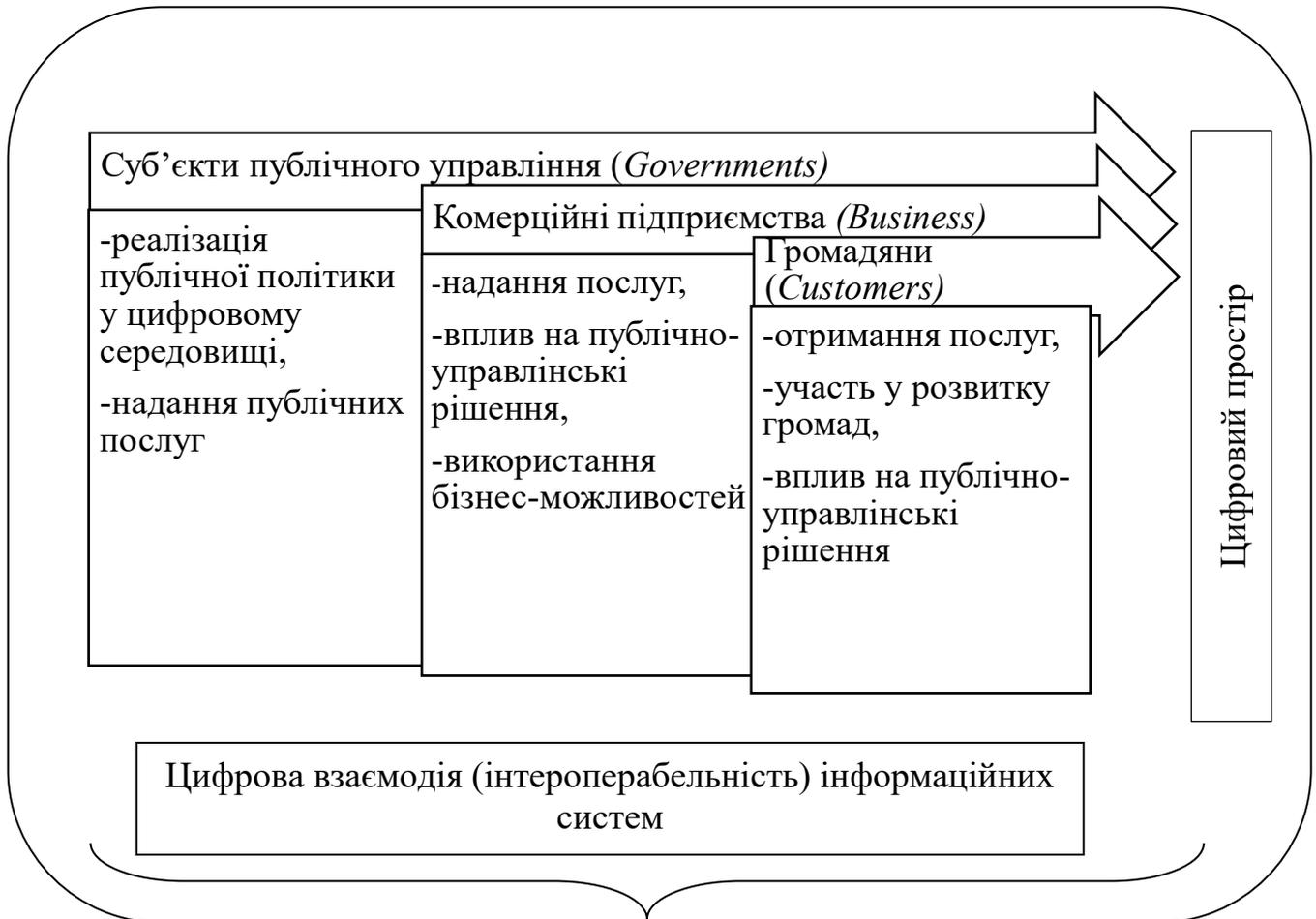


Рис. 1.2 - Суб'єкти інформаційно-цифрового простору

Джерело: складено автором

Інноваційний розвиток інформаційно-комунікативних і цифрових технологій сприяє формуванню широкого спектра інструментів, що забезпечують участь громадян в управлінських процесах на місцевому, національному та глобальному рівнях. Сучасні технологічні рішення створюють нові цифрові платформи для підвищення прозорості даних, розширення доступу до інформації, здійснення громадського моніторингу, підзвітності та оцінювання якості публічних послуг, водночас активізуючи залучення громад і громадян до

процесів прийняття рішень. Територіальні громади використовують безліч засобів для доступу та обміну інформацією, формуючи «комунікативну екологію», коли люди роблять вибір щодо інструментів, які найкраще відповідають їхнім потребам та контекстам. Технології варіюються від радіо спільноти, служб коротких повідомлень (SMS), додатків для мобільних телефонів, голосових звітів, веб-сайтів, соціальних медіа та інтерактивного картографування тощо [29]. У цьому зв'язку узагальнимо основні завдання, які вирішуються шляхом інформаційного обміну (рис 1.3).

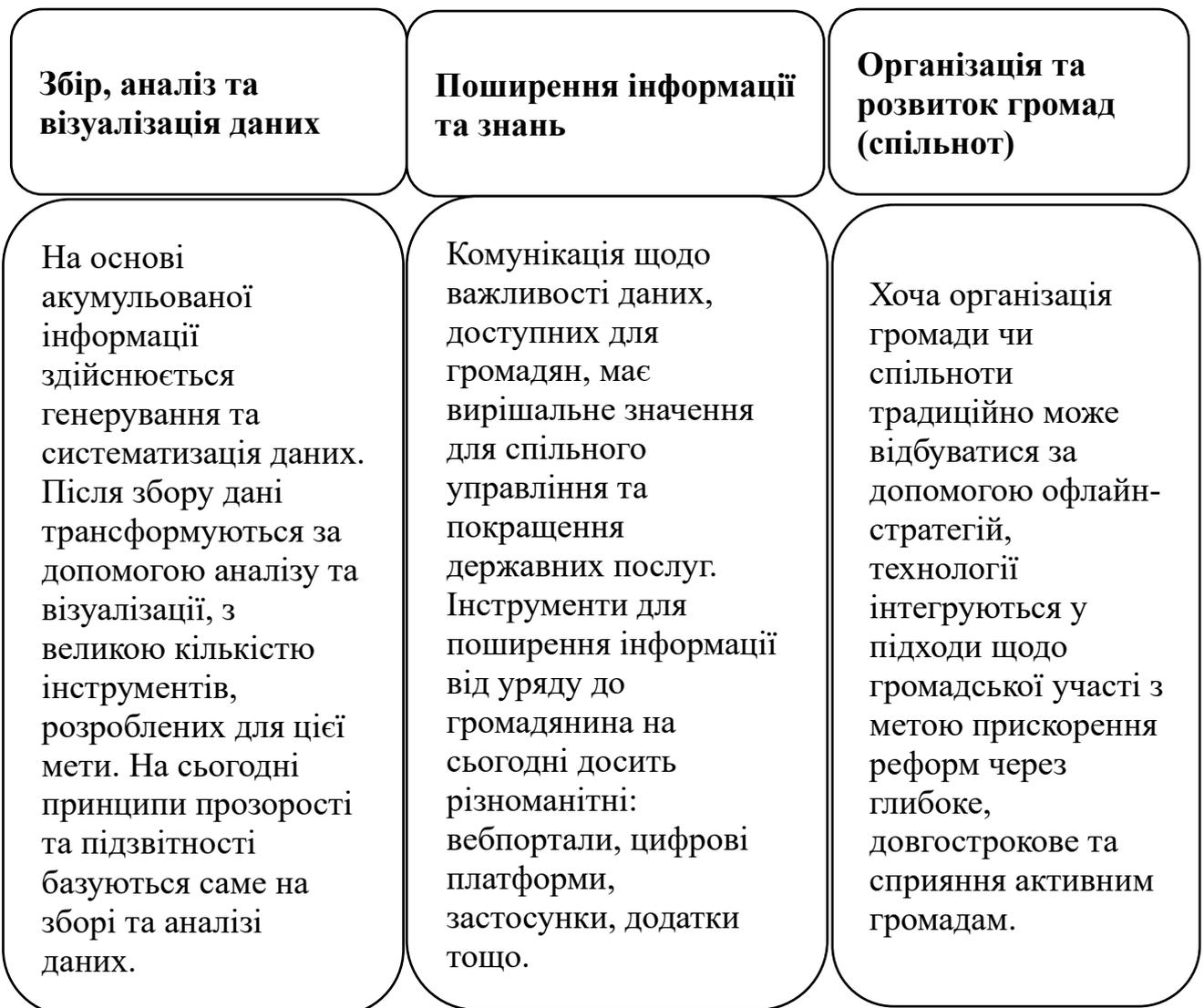


Рис. 1.3. Основні завдання, які вирішуються шляхом інформаційного обміну

Джерело: узагальнено автором

Принагідно зазначимо, що відсутність комунікації тягне за собою розбалансування єдності цілісного формування влади як органічного явища. Органічного, тому що нинішня система влади є досить тонкою матерією, абсолютно чутливою до викликів і загроз, а тому такою, що діє вже не як механізм, а як цілісна система. Така органічність робить процеси інформаційного обміну надзвичайно важливими, оскільки вони об'єднують цю систему як організовану сукупність елементів та інтегрують її можливості, що дозволяє робити висновки, що цифрова взаємодія та інтеперабельність інформаційних систем органів публічної влади набирає потужних обертів.

Останнім часом термін «інтеперабельність» як механізм цифрової взаємодії інформаційних систем, набуває популярності, привертаючи увагу професіоналів і дослідників найрізноманітніших сфер. Однак це не означає, що він є досить новим. Згідно з хронологією історичного видання Webster's Timeline History, термін використовувався десятиліттями у таких сферах, як армія, транспорт, охорона здоров'я, громадська безпека, зв'язок та інформатика [30, с. 16].

Оксфордський словник англійської мови тлумачить інтеперабельність як сумісність (між/з чимось) та здатність комп'ютерних систем, платформ, програм обмінюватися інформацією. Ця нова функція покликана забезпечити кращу взаємодію між пристроями та інформаційними системами [31].

Інтеперабельність інформаційних систем вважається обов'язковою для досягнення успіху компаній і навіть для їх виживання в поточному мережевому і глобалізованому світі, оскільки це забезпечує підвищення їх гнучкості та конкурентоспроможності, дозволяє надавати більш інтегровані послуги, зменшує експлуатаційні витрати та покращує ефективність роботи. Разом з тим, визнано, що досягнення інтеперабельності інформаційних систем є досить складним завданням.

Концепція інтеперабельності (сумісності) інформаційних систем передбачає також автономність у роботі та пов'язується із поняттями «взаємодія» та «інтеграція», які часто використовують як синоніми сумісності.

Однак, як зазначають дослідники, автономність роботи інформаційних систем є фундаментальною і, отже, здатність створювати взаємодію між системами має бути досягнуто з мінімальним втручанням у автономність кожної з них.

В основу концепції сумісності П. Міллер (Paul Miller) відносить набір ключових ідей – «дві або більше інформаційних системи юридичних осіб, які працюють разом», «спільне розуміння», «безпроблемна робота», «операція зі спільною метою», «автономія» та пропонує розуміти сумісність як здатність двох і більше різнорідних і автономно діючих суб'єктів обмінюватися і використовувати інформацію або функції один одного, правильно, зручно і без істотних зусиль з метою досягнення конкретних цілей.

Згідно з цими уявленнями використання терміну «сумісність» стосується ситуацій, коли системи розроблені ізольовано, діючи незалежно, однак, демонструючи різні характеристики, вони здатні функціонувати спільно для досягнення загальної мети, із збереженням їх автономності [32].

Концепція сумісності пов'язується також із терміном «інтеграція». Стандартний словник термінів з електротехніки та електроніки американського Інституту інженерів з електротехніки та електроніки (IEEE - Institute of Electrical and Electronics Engineers) термін «інтеграція» тлумачить як «процес комбінування програмних компонентів, апаратних компонентів або їх разом у загальній системі» або як «злиття чи об'єднання двох або більше елементів нижчого рівня в єдиний елемент вищого рівня для забезпечення роботи функціональних та фізичних інтерфейсів» [33].

Онлайн-словник Merriam-Webster Британської енциклопедії термін «інтегрувати» пояснює як «формувати, координувати, змішувати у функціонуюче чи єдине ціле», «об'єднуватися з чимось іншим» або «об'єднати у більшу одиницю» [34].

Інтеграція розглядається як процес комбінування з виходом за межі взаємодії та складної заміни елементів системи, вона передбачає створення єдиного цілого, де елементи настільки тісно переплітаються, що їхня заміна стає складним інженерним або організаційним викликом, який часто потребує

перебудови всієї архітектури. На противагу цьому, інтероперабельність (сумісність) виступає як динамічна здатність автономних суб'єктів до ефективної взаємодії через стандартизовані інтерфейси.

У цьому сенсі можна сказати, що інтегровані системи повинні бути сумісними, але інтероперабельні системи не обов'язково повинні бути інтегровані. Основна відмінність понять «інтероперабельність» та «інтеграція» наведена у табл. 1.4.

*Таблиця 1.4*

Основна відмінність понять «інтероперабельність» та «інтеграція»

<b>Інтероперабельність інформаційних систем</b>	<b>Інтеграція інформаційних систем</b>
Співіснування	Уніфікація
Автономність	Асиміляція
Легка заміна	Складна заміна

Джерело: узагальнено автором за [32].

На відміну від того, що відбувається при повній інтеграції, в якій зв'язки між системами жорсткі і фіксовані, при інтероперабельності зв'язки між системами є більш гнучкими, їх легко встановити та змінити.

Отже, перебуваючи в режимі цифрової взаємодії, інформаційні системи суб'єктів-учасників (органів публічної влади) залишаються автономними та незалежними, а будь-який з компонентів може бути легко замінений або доповнений іншим із потрібними специфікаціями без зміни функціональності в цілому. Це означає, що процес розвитку електронного урядування шляхом запровадження цифрової взаємодії інформаційних систем органів публічної влади за принципом інтероперабельності дозволить здійснювати реалізацію сервісно-орієнтованої публічної політики без зривів, гальмування та форсмажорних обставин.

Підсумовуючи аналіз ключових понять дослідження, зазначимо, що

електронне урядування продовжує привертати увагу світової спільноти завдяки своїй здатності зробити уряди більш ефективними та результативними, а отже, трансформувати відносини з громадянами, бізнесом та органами публічної влади на засадах оперативності, якості, дотримання прав та задоволеності громадян, як того вимагають реалії сучасного цифрового суспільства.

## **1.2 Історичні основи розвитку інформаційних систем, цифрової сумісності та взаємодії органів публічної влади**

Сучасний світ стрімко зазнає змін: розширюються можливості цифрової взаємодії, інтенсивно розвивається електронне урядування, поширюються віртуальні форми організації діяльності, удосконалюються процеси та алгоритми надання адміністративних послуг. Сукупність цих змін зумовлює необхідність формування ефективної інформаційно-цифрової архітектури суб'єктів публічного управління, здатної забезпечити підвищення якості життя населення та зміцнення соціального добробуту. Водночас цифрові трансформації стимулюють економічну активність, розвиток демократичних практик і міжінституційної взаємодії на національному й місцевому рівнях, що сприяє зростанню суспільної довіри до органів публічної влади.

Світ змінюється, змінюються разом з ним люди, розвиваються технології. Поглиблення технологічного розвитку та його інтеграція у повсякденні соціальні процеси зумовили появу на межі тисячоліть нового концепту в теорії та практиці публічного управління – взаємодії інформаційних систем органів публічної влади та забезпечення їх цифрової сумісності (інтероперабельності), що актуалізує потребу у даному дослідженні.

У міру того, як протягом історії розвиток технологій запису та обробки інформації поступово відкривав нові можливості для їх застосування. Винахід друкарського верстата Йоганном Гутенбергом у середині XV століття та створення механічного калькулятора Блезом Паскалем у XVII столітті є яскравими прикладами таких технологічних проривів. Ці інновації спричинили

радикальні зміни у способах фіксації, обробки, поширення та отримання інформації й знань, що, у свою чергу, глибоко вплинуло на управління суспільним розвитком, організацію комерційної діяльності та повсякденне життя окремих людей [35].

Першою великомасштабною механічною інформаційною системою вважається Табулятор перепису Германа Холлерита. Створена для обробки перепису населення США 1890 року, ця машина стала ключовим етапом автоматизації обробки даних і надихнула подальший розвиток комп'ютеризованих інформаційних систем [36].

Одним з перших комп'ютерів, що використовувалися для такої обробки інформації, був UNIVAC I, встановлений в Бюро перепису населення США в 1951 році адміністративних цілей та в компанії General Electric у 1954 році для комерційного використання. З кінця 1970-х років персональні комп'ютери надали нові можливості інформаційних систем малим підприємствам і приватним користувачам.

На початку того ж десятиліття глобальна мережа Інтернет, яка почала активно розвиватися на початку 1980-х років. У 1991 році Всесвітня павутина, створена Тімом Бернерсом-Лі для доступу до взаємопов'язаної інформації, розміщеної на численних комп'ютерах у глобальній мережі, запрацювала як основна служба Інтернету. Широке поширення Інтернету та веб-технологій забезпечило безпрецедентний доступ до інформації, ресурсів і створило нові можливості для взаємодії людей та організацій [37].

Прогрес електронної комерції через Інтернет обумовив суттєве зростання цифрових міжособистісних комунікацій, зокрема через електронну пошту та соціальні мережі, а також масове поширення цифрових продуктів (програмного забезпечення, музики, електронних книг і фільмів) та здійснення ділових операцій в онлайн-середовищі (купівля, продаж, реклама). Поширення смартфонів, планшетів, ноутбуків та інших мобільних пристроїв із доступом до бездротових мереж забезпечило функціонування інформаційних систем як інструменту мобільності, що стає невід'ємною складовою повсякденного життя

людини.

Оскільки інформаційні системи уможливили більш різноманітну людську діяльність, вони вплинули й на суспільні відносини. Ці системи прискорили темп повсякденної діяльності, дозволили людям розвивати і оперативно підтримувати комунікацію, вплинули на структуру і склад організацій, додали функціоналу органам влади.

Історія новітніх інформаційних систем (ІС) налічує трохи більше шести десятиліть. Водночас їх поява та розвиток у глобальному масштабі сприяли прискоренню автоматизації управлінських процесів у всіх сферах суспільного життя, від комерційної діяльності до публічного управління, здійснивши, можливо, наймасштабніший вплив серед усіх технологічних досягнень світової історії. Сьогодні основу функціонування ІС становлять Всесвітня павутина, Інтернет або будь-яка локальна мережа органів влади чи підприємств.

Близько шістдесяти років тому світова ділова сфера переживала безпрецедентне зростання. Значна частина досвіду, який стимулював економічний розвиток, була здобута під час Другої світової війни, коли промислові потужності багатьох держав були перетворені на високоефективні військові виробничі системи.

Період Другої світової війни також позначився появою перших комп'ютерів, так званих машин Т'юрінга, які використовувалися для розшифрування німецьких кодів і завчасного інформування союзників про переміщення противника [38].

За сучасними мірками ці ранні комп'ютери були досить громіздкими, дорогими (вартість сягала півмільйона доларів) і значно поступалися за потужністю навіть сучасним калькуляторам у смартфонах. Проте вони відкрили фахівцям шлях до створення більших і складніших систем, які в бізнесі та промисловості дозволяли ефективніше перетворювати капіталовкладення на прибуткові підприємства і згодом отримали назву інформаційних систем.

До середини 1960-х років ІС увійшли у мейнстрім бізнесу. У той час, коли комп'ютери залишалися недоступними для більшості організацій через високу

вартість, телекомунікаційні процеси здійснювалися за допомогою системи TELEX. Це забезпечувало підприємствам можливість оперативного обміну інформацією в межах організації з будь-якої точки світу і в будь-який час [39].

Використання інформаційних систем у бізнесі та промисловості зазвичай починалося з бухгалтерських відділів. У 1970-х роках керівники підприємств усвідомили важливість ІС та ту гнучкість, яку вони надавали бізнес-процесам. TELEX став стандартом передачі даних, а мейнфрейми – потужні комп'ютери для обробки великих обсягів інформації – використовувалися для створення баз даних. Поступово потреба в структурованому та легкодоступному зберіганні інформації сприяла розширенню застосування мейнфреймів на управлінські функції компаній, а не лише на бухгалтерію. Згодом, коли інформаційні системи отримали власну автономію та значні бюджети в корпораціях, розпочалося активне інвестування у складні та динамічні системи та програмне забезпечення [40].

Поява міні- та мікрокомп'ютерів спричинила новий етап розвитку ІС, зокрема через впровадження електронної пошти, що дозволяла передавати інформацію без використання мейнфреймів та забезпечувала автономну комунікацію між користувачами.

Однак постачальники програмного та апаратного забезпечення вимагали від бізнесу зміни стилю ведення бізнесу, щоб він відповідав комп'ютерним системам. У той час стандартизація апаратних і програмних рішень була недостатньою, і багато молодих компаній зазнавали банкрутства через відсутність технічної або системної підтримки, адже впровадження нових систем, що значно перевищували бюджет, спричиняло великі фінансові витрати.

Потреба підтримки роботи підприємств за допомогою ІС та зростання доступності апаратного й програмного забезпечення зумовили розробку власних програм і алгоритмів управління інформаційними системами. Внаслідок цього в організаціях з'явилася нова посада - директор з інформаційних технологій, яка в багатьох компаніях того часу за значенням прирівнювалась до генерального директора. Основними функціями цієї посади були стандартизація всіх

інтерфейсів електронних даних між підрозділами, уніфікація інформації та забезпечення її ефективного використання [41].

У середині 1980-х років більшість виробничих компаній почала впроваджувати інформаційні системи для прогнозування продажів, обробки замовлень та управління розподілом продукції. У 1989 році Тім Бернерс-Лі створив World Wide Web – HTML-протокол, який відкрив нову еру технологічного розвитку, безпрецедентну для того часу. До середини 1990-х років стало очевидним, що жодна корпорація не може ефективно функціонувати без надійної ІС та інтеграції з постачальниками й дистриб'юторами в ланцюзі поставок [42].

Таким чином, без інформаційних систем сучасний розвиток усіх сфер суспільного життя був би неможливим. Протягом останніх 50 років ІС перетворилися на фундамент управлінських процесів, а принципи застосування та алгоритми роботи, створені в 1960-х і 1970-х роках, залишаються актуальними й сьогодні в публічному управлінні. Отже, аналіз еволюції інформаційних систем ХХ століття свідчить: 1960-1970-ті роки – це десятиліття організаційних мейнфреймів і міні-обчислень із спільним використанням даних; 1980-ті – епоха персональних комп'ютерів без обміну інформацією; 1990-ті – період розвитку мереж із організаційними обчисленнями та активним обміном даними (табл. 1.5).

*Таблиця 1.5*

Еволюційний розвиток інформаційних систем ХХ сторіччя

1960-ті та 1970-ті роки	Розвиток організаційних мейнфреймів та міні-обчислень із спільним використанням даних
1980-ті роки	Розбудова персональних комп'ютерів без обміну даними
1990-ті роки	Розширення мереж з організаційними обчисленнями та обміном даними

Джерело: узагальнено автором за [37-42]

Матеріали Генеральної Асамблеї ООН 1994 року підкреслюють визнання важливості інформаційних технологій, що визначає розвиток інтегрованих інформаційних систем управління як засіб стимулювання їх поширення та застосування у державному секторі [43].

Інформаційні системи з часом зазнали значної еволюції. Їх активне впровадження в управлінських процесах і різних сферах діяльності не лише підвищило ефективність адміністративної роботи, але й забезпечило конкурентні переваги. Інтеграція комп'ютерних технологій та комунікацій стала невід'ємною тенденцією застосування цифрових рішень у XXI столітті.

Технологічний розвиток третього тисячоліття свідчить, що швидке поширення інформаційних систем, розвиток мов програмування та повсюдна цифровізація визначатимуть майбутні напрями технологічного зростання. Серед функціональних можливостей, які можуть бути впроваджені найближчим часом, передбачається управління життєвим циклом продукту, зберігання даних, системи управління знаннями та збалансована система показників. Всі ці компоненти поступово інтегруватимуться в єдину систему для сприяння розвитку новітніх ІС. Очікується також, що існуючі функціональні можливості будуть значно вдосконалені, а ключові цифрові тенденції включатимуть використання відкритого програмного забезпечення та мобільних додатків у сфері мобільної комерції. Крім того, прогнозується повна інтеграція мобільних пристроїв з інформаційними системами [44].

Сучасні тенденції розподіленої обробки та мережевих обчислень формують принципово інші стратегії розвитку державних інформаційних систем порівняно з підходами 1970-х та 1980-х років. Нині робочі станції, розподілена обробка та мережеві обчислення з активним обміном ресурсами й даними стали ключовими елементами державних ІС та повсюдної цифровізації. Такий підхід особливо вигідний для країн, що розвиваються, оскільки він забезпечує низькі витрати, мінімальні ризики та високі можливості для впровадження високотехнологічних стратегій у сфері публічного управління.

З іншого боку, поява доступних та високопродуктивних мікрокомп'ютерів і супутніх технологій перетворила державні інформаційні системи на ключові інструменти функціонування органів публічної влади. Сучасна конкурентоспроможність у глобальній економіці вже не обмежується низькою вартістю робочої сили, а значною мірою визначається здатністю впроваджувати

передові технології для генерації, обробки та передавання інформації. Водночас зростання інформаційно-цифрової інтенсивності діяльності та існуючі диспропорції у використанні цифрових технологій між індустріально розвиненими країнами та країнами, що розвиваються, ймовірно, сприятимуть поглибленню розриву між «інформаційно багатими» та «інформаційно бідними» економіками. Події останніх років, зокрема пандемія COVID-19 та воєнний стан в Україні, підтвердили критичну роль ефективної роботи органів публічної влади у забезпеченні своєчасного надання адміністративних послуг, захисту прав громадян та задоволенні базових потреб у сферах освіти, охорони здоров'я та зайнятості [45].

У контексті дослідження еволюції інформаційних систем публічного управління варто згадати концепцію «New Public Management» (новий публічний менеджмент) 1980–1990-х років, яка поступово трансформувалася в електронне урядування. Ключові напрями тогочасного підходу включали: а) дезагрегацію як децентралізацію управлінських повноважень та розвиток локальних інституцій місцевого значення; б) конкуренцію як появу альтернативних постачальників послуг, скасування монополій, розвиток аутсорсингу та продаж активів; в) мотивацію як стимулювання діяльності підприємств через ефективне використання ресурсів і часу, розвиток державно-приватного партнерства та кореляцію рівня оплати з якістю виконання робіт [46].

Відомо, що інформаційні системи становлять основу електронного урядування. Аналізуючи історичний розвиток електронного урядування в Україні, слід зазначити, що впровадження новітніх систем електронного голосування в органах публічного управління передбачає фіксацію та обробку результатів волевиявлення депутатів під час прийняття рішень. Оскільки такі системи здебільшого базуються на інформаційних технологіях та обчислювальній техніці, вони потенційно можуть стати об'єктом злочинних посягань. Фальсифікація результатів голосування через порушення роботи електронних систем може перешкоджати ефективному вирішенню загальнодержавних та місцевих соціально-економічних, екологічних проблем і

справедливому розподілу ресурсів (земельних, водних, корисних копалин тощо) територіальних громад [47]. На місцевому рівні, особливо в районних радах, подібні системи взагалі відсутні.

Поглиблення цифрових навичок громадян та розвитку електронного спілкування сприяє підвищенню їх обізнаності щодо принципів функціонування інструментів електронної демократії, можливості впливати на політичні процеси, законодавчі інновації та брати участь у прийнятті рішень на відповідній території. Загалом, незважаючи на існуючі недоліки та економічні складнощі, у світі дедалі ширше впроваджуються системи електронного голосування (наприклад, бюджет участі), які стають важливою складовою концепції електронного уряду.

Інтернет та пов'язані з ним технології стали важливими інструментами забезпечення економічної та соціальної активності під час запровадження правового режиму воєнного стану. У цьому контексті цифрова політика набуває особливої актуальності, оскільки здатна як максимізувати нові можливості, так і зменшувати негативні наслідки кризових ситуацій. Відповідно, цифровізація суспільного життя та формування цифрового порядку денного мають стати основою планів і стратегій економічного розвитку та поствоєнного відновлення [48]. Це зумовлює потребу розробки програм розвитку, що базуються на цифровій трансформації, і свідчить про рух світу до нової ери цифрових порядків денних.

У 2003 і 2005 роках Всесвітній саміт з питань інформаційного суспільства закликав до активного впровадження інформаційно-комунікаційних технологій як інструментів цифрового розвитку. Це стимулювало країни до створення порядку денного цифрового суспільства, орієнтованого на скорочення цифрового розриву, розвиток електронного урядування та підвищення обізнаності щодо можливостей новітніх технологій [49]. У цьому контексті доцільно виділити історичні етапи розвитку інформаційних систем XXI століття (рис. 1.4), які ілюструють перехід від інформаційного до цифрового суспільства, свідками якого є сучасне покоління.



Рис. 1.4. Періодизація розвитку інформаційних систем ХХІ сторіччя

Джерело: складено автором

Таким чином, існує принаймні три підстави, що визначають вирішальну

роль ефективного застосування інформаційних систем та цифрових технологій у процесах публічного управління для досягнення економічних і соціальних цілей.

По-перше, з огляду на економічну вагу державного сектору та органів місцевого самоврядування в будь-якій країні, підвищення продуктивності їхньої діяльності приносить значні вигоди для національної економіки в цілому. Відомо, що публічний сектор формує суттєву частку зайнятості, кінцевих споживчих витрат та валового внутрішнього накопичення основного капіталу.

По-друге, публічне управління є найбільшим і найширшим збирачем публічних даних та інформації. Ці ресурси охоплюють бази даних, що включають економічну та соціальну діяльність, а також природні та географічні ресурси.

По-третє, у контексті глобальної економіки, насиченої інформацією, ефективні державні інформаційні системи забезпечують доступ до міжнародних баз даних і світових знань, що сприяє прозорому та результативному публічному управлінню та адмініструванню у світовому політичному просторі.

Сьогодні, враховуючи зростаючу цифровізацію в усіх сферах суспільного розвитку, залежність від онлайн-систем та управління даними, органи публічної влади поступово переходять на хмарні технології. Це підвищує ефективність роботи, знижує навантаження на ІТ-відділи органів публічної влади, підвищує гнучкість та знижує накладні витрати.

Хмарна інтероперабельність – це здатність або ступінь, у якому одна хмарна служба пов'язана з іншою шляхом обміну даними відповідно до прийнятих обома сторонами стратегії, стандартів, протоколів для отримання результатів. Перевагами такого застосування є: а) можливість аварійного відновлення, яке є простіше та дешевше, аніж заміна серверів; б) розширення співробітництва під час роботи з одним документом – хмарні технології оптимізують робочий процес і роблять обмін файлами простіше і безпечніше, ніж будь-коли раніше; в) віддалений доступ; г) забезпечення урядовим установам безпекового рівня, який був недосяжний під час використання внутрішніх ІТ-систем; д) конкурентоспроможність: державні установи мають

бути в курсі інноваційних технологій, і хмара може допомогти їм у цьому; е) економія: скорочення витрат та розширення потужностей без додавання серверів; є) екологічність: зниження витрат на електроенергію та споживання менше ресурсів, ніж традиційні аналоги [50].

Окрім того, поступово набирає обертів розвиток туманних технологій. Відомо, що кількість інформації, яка у великих обсягах обертається в інформаційних системах, постійно збільшується. Відтак питання ефективних технологій зберігання та обробки даних постійно залишається актуальним. На зміну чи на додаток до хмарних технологій все більшої популярності набуває новий тренд у хмарних обчисленнях під назвою «туманна технологія» (*fog technology*), коли інформація надходить користувачам не через єдине фізичне хмарне сховище, а через географічно розподілені платформи.

«Туманна технологія» – це удосконалена хмарна технологія, головною особливістю якої є розподіл обчислень між пристроями, які є складовою Інтернету речей (зокрема, смартфонами, та іншими пристроями, підключеними до Інтернету, якими сьогодні користується майже кожен). При використанні технології *fog* вторинні дані створюються з використанням спільних ресурсів і завжди передаються в хмару на віддалені сервери. Туманні технології можуть забезпечити абсолютно новий сервіс у наданні адміністративних послуг (можуть надаватись у центрах обробки даних або на кінцевих вузлах мережі), оскільки наділені можливістю розподіляти засоби комунікації, обчислювальні ресурси, сервіси, засоби управління та зберігання тощо. Туманні технології значно поліпшують можливість хмарних сервісів з огляду на можливість обробки даних на кінцевих пристроях мережі (а не на центральному сервері), тим самим забезпечуючи безпеку передачі даних та зменшуючи ризики втрат інформаційної бази даних.

Підсумовуючи зазначимо, що інновації мають вирішальне значення для майбутнього добробуту суспільства та стимулювання економічного зростання. Не лише хмарні чи туманні технології найближчим часом будуть широко впроваджуватись у контексті розвитку електронного урядування та цифровізації.

Джим Рікотта, керівник компанії Aliro Quantum, на Всесвітньому економічному форумі у травні 2022 року зазначив, що протягом наступних п'яти років квантовий Інтернет здійснить революцію в світі подібно до того, як класичний Інтернет трансформувалася суспільство минулого століття. Подібно до того, як класичні мережі створили сучасний Інтернет, квантові мережі стануть основою квантового Інтернету майбутнього. Передбачається, що він матиме значний вплив на різні сфери життя, сприяючи проривам у енергетиці, медицині, матеріалознавстві та інших галузях. За прогнозами, до 2027 року квантові мережі з локальних мереж і кластерів розвинуться до рівня континентальних систем [51].

Стратегічна програма ЄС на 2030 рік «Шлях до цифрового десятиліття» встановлює конкретні цифрові цілі на основі чотирьох основних завдань: цифрові навички, цифрова інфраструктура, цифровізація бізнесу та цифровізація адміністративних послуг. Амбітні цілі спрямовані на забезпечення безпечного доступу всіх громадян та підприємств до державних послуг в Інтернеті: 100% онлайн-надання ключових державних послуг, доступних для громадян та підприємств Європи, 100% громадян Європи надано доступ до медичних записів (електронні записи), а 80% громадян використовують форму цифрового посвідчення особи. Хоча існують значні відмінності в процесах і рівнях цифровізації в різних державах, дані показують, що більшість держав-членів, які 5 років тому мали нижчий рівень цифровізації, просуваються вперед швидшими темпами, ніж інші, що свідчить про спільне зближення до цих цілей цифровізації в ЄС [52].

Тож цілком очевидно, що публічне управління в Україні не може бути продуктивним, результативним та ефективним без технологічної підтримки. Використання новітніх інформаційних та цифрових технологій є абсолютною вимогою для розвитку електронного урядування в Україні та побудови сервісно-орієнтованої держави.

### **1.3 Стан наукових досліджень проблем цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування**

Цифрова взаємодія інформаційних систем (інтероперабельність) протягом майже чотирьох десятиліть у різних галузях. Питання цифрової взаємодії суб'єктів управління активно обговорюється як у зарубіжній науковій літературі, так і вітчизняними дослідниками, як з техніко-технологічної, так і з соціогуманітарної перспективи. Відомо, що цифрові платформи становлять складний об'єкт дослідження через їхню розподілену природу та взаємопроникнення з технологіями, функціональними процесами, програмним забезпеченням та соціотехнічними аспектами тощо.

Сучасні технологічні підходи, такі як концепції «розумних міст», «розумної мобільності» та «розумних будинків», ґрунтуються на мережі взаємопов'язаних фізичних пристроїв, здатних автоматично обмінюватися даними. Аналогічна технологічна парадигма застосовується для забезпечення інтероперабельності інформаційно-аналітичних систем органів публічної влади, що створює умови для формування сервісно орієнтованої державної політики. Розвиток цих систем сприятиме фундаментальним трансформаціям у економічній, технологічній та соціальній сферах як для громадян, так і для держави.

Німецький дослідник Д. Ходап (Daniel Hodapp) відзначає, що сучасні дослідження здебільшого зосереджуються на вивченні переваг цифрових інновацій. Водночас їхнє ефективне впровадження значною мірою залежить від ключової передумови: технічної, технологічної, функціональної та семантичної сумісності інформаційних систем. Цей термін визначається як здатність двох або більше систем обмінюватися даними, аналізувати та генерувати інформацію, що забезпечує коректну циркуляцію даних у мережах. Науковець зазначає, що проблема сумісності нині виходить на новий рівень, оскільки цифрові інновації охоплюють нові, значно менш стандартизовані сфери, ніж класичні цифрові середовища, де домінує єдина платформа-лідер, наприклад iOS від Apple [53, с.

408]. Аналогічні виклики спостерігаються й у контексті цифрової взаємодії інформаційних систем органів публічної влади.

З точки зору інформаційних систем (ІС), про які велась мова у попередньому розділі, загально визнано, що сумісність у межах локальних цифрових екосистем має суттєвий вплив на розвиток інновацій, конкуренцію та створення доданої вартості всієї екосистеми на рівні окремої країни або групи країн.

Показово, що численні суб'єкти управління, як комерційні, так і неприбуткові, інвестують значні фінансові ресурси для підвищення сумісності інформаційних систем. Так, у 2021 році великі телекомунікаційні компанії створили платформу OCF (Open Connectivity Foundation) з метою уніфікації підключення промислових пристроїв. Така стандартизація відкриває нові інноваційні та безпечні можливості використання, зменшує витрати на розробку, спрощує інтеграцію та скорочує час виходу на ринок, а також полегшує дотримання нормативних вимог щодо базових рівнів безпеки й конфіденційності та покращує користувальницький досвід [54].

У науковому дискурсі сучасні дослідження зосереджені на кількох ключових напрямках: виявленні деструктивних факторів, що ускладнюють розбудову інтероперабельності систем; розвитку новітніх цифрових платформ, здатних адаптуватися до взаємодії з іншими платформами та системами для ефективного управління; а також моделюванні перспектив їхнього розвитку на майбутнє.

Перший аспект дослідницької уваги стосується деструктивних чинників, які спричиняють низьку цифрову сумісність, неефективну координацію стандартів та технологічну турбулентність. Інакше кажучи, поява численних нових стандартів або платформ у межах екосистеми призводить до використання різних підходів для досягнення сумісності [55]. Д. Тіс (David J. Teece), американський організаційний економіст, професор глобального бізнесу Каліфорнійського університету та директор Центру управління інтелектуальним капіталом Ташера у Школі бізнесу У. Хааса, виділяє кілька причин низької

сумісності інформаційних систем: а) впровадження нових та більш гетерогенних інформаційних технологій; б) швидке зближення раніше відокремлених кіберфізичних екосистем; в) залучення різноманітних акторів, таких як виробники апаратного забезпечення, ІТ-компанії, малі стартапи та зацікавлені державні суб'єкти [56].

Другий аспект досліджень зосереджений на механізмах підвищення цифрової сумісності, тобто на інструментах, які сприяють ефективній взаємодії систем. Як показує аналіз наукової літератури, такими механізмами є стандарти та платформи. Вони впливають на різні архітектурні рівні, забезпечуючи семантичну та синтаксичну сумісність даних, що дозволяє розподіленим системам уніфіковано читати та інтерпретувати інформацію. Ключовими характеристиками цифрових технологій, які також повинні розвиватися у взаємодії, є конвергенція та генеративність. Конвергенція означає злиття раніше розділених просторів цінностей, тоді як генеративність визначається як здатність технологій спричинити раптові зміни під впливом великої, різноманітної та скоординованої аудиторії. Поєднання цих двох властивостей є необхідною умовою для реалізації процесів інтеперабельності [57]. Отже, акцент сучасних досліджень робиться не стільки на досягненні цифрової сумісності самої по собі, скільки на посиленні генеративності платформ, використовуючи сумісність як стратегічний ресурс. У цьому контексті важливою концепцією є відкритість платформ, що розглядається як технічна сумісність платформи з іншими системами або платформами на тому ж чи іншому архітектурному рівні. Додатково, концепція відкритості ресурсів пов'язується з забезпеченням оперативної сумісності [58].

Третій напрям досліджень зосереджується на оцінці результатів застосування механізмів цифрової сумісності та спрямований на формування уявлення про ті переваги та перспективи підвищення сумісності, які слід активно використовувати, а також про ті, які не є доцільними для впровадження. Основні напрями наукових досліджень цифрової сумісності інформаційних систем наведено на рис. 1.5.

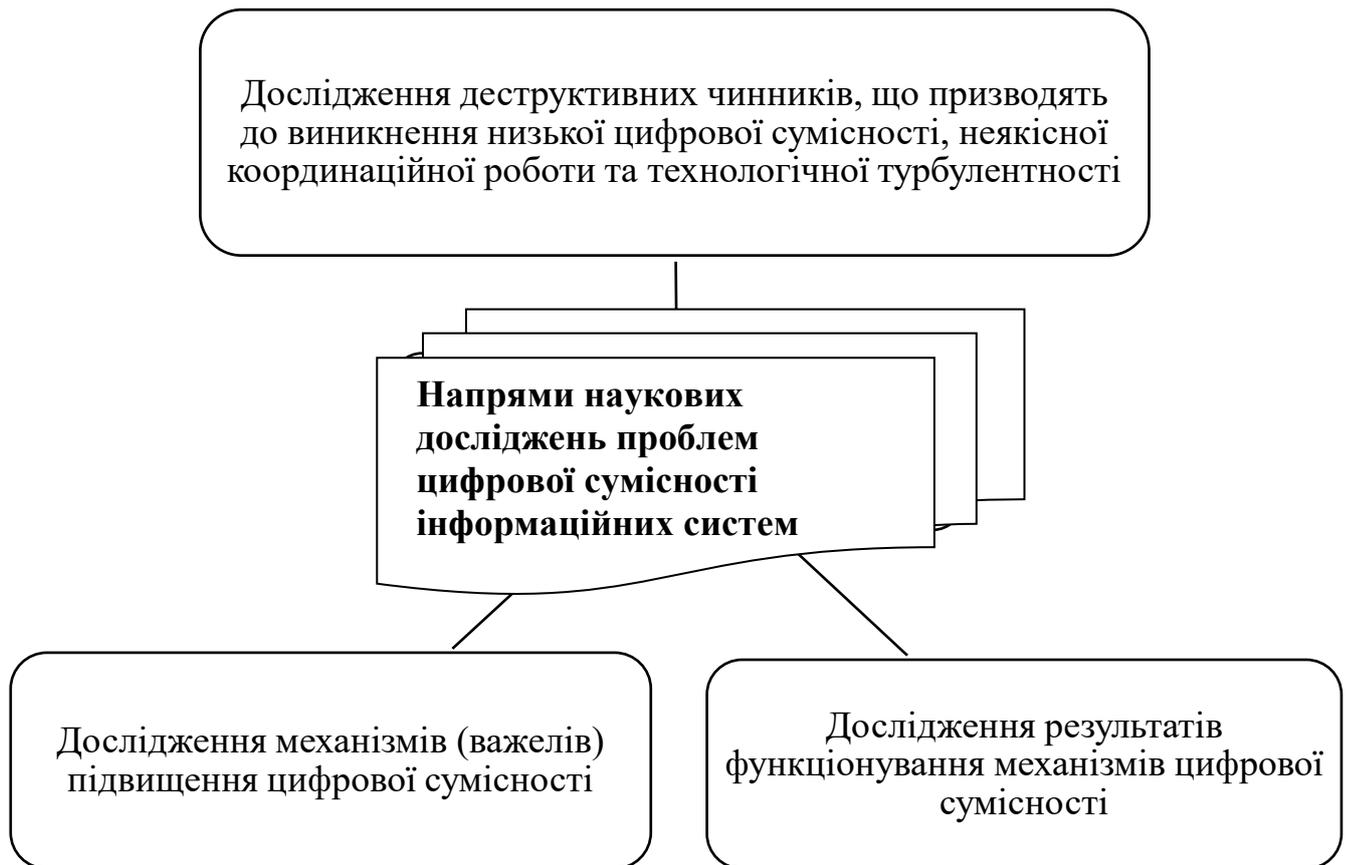


Рис. 1.5. Основні напрями наукових досліджень цифрової сумісності інформаційних систем

Джерело: власна розробка автора

Що стосується переваг і перспектив цифрової сумісності, можна виділити кілька основних аспектів.

По-перше, цифрова сумісність сприяє розвитку нових і більш досконалих інновацій. Поліпшена сумісність інформаційних систем дозволяє моделювати програмні компоненти так, щоб вони взаємодіяли за визначеними стандартами, що спрощує їх інтеграцію та спільне використання з іншими системами [59].

По-друге, підвищення сумісності стимулює конкуренцію, зменшуючи випадки блокування та знижуючи бар'єри для входу на ринок [56].

По-третє, більш високий рівень сумісності підсилює автономію користувачів та організацій. У сумісних системах вони можуть обирати серед конкурентних і взаємодоповнюючих варіантів ті, що швидко тестуються під конкретні потреби, без обмежень попередніх технологій [60, с. 189].

По-четверте, цифрова сумісність полегшує доступ до інформації та знижує транзакційні витрати, за умови наявності трьох складових: прозорості та справедливої моделі управління, економічних стимулів для всіх учасників та надійної технологічної інфраструктури для безпечного підключення нових суб'єктів [61].

Водночас існують і ризики. Хоч широке впровадження платформ і стандартів стимулює інновації, надмірне концентрування користувачької бази може призвести до монополізації, що обмежує конкуренцію і потенційно гальмує подальший розвиток цифрових інновацій.

Як зазначалось у підрозділі 1.1 роботи, визначення цифрової взаємодії інформаційних систем формується науковцями, базуючись на різних підходах. Наприклад, розробка стандартів, платформ, ключових механізмів для забезпечення взаємодії, є, по суті, технічним завданням, яким займаються дослідники технічного спрямування майже 40 років. Дослідницькі роботи з питань цифрових інновацій містять думку про те, що розвиток технологій і пов'язаних з ними знань, необхідних для впровадження інновацій, досягла на сьогодні безпрецедентних висот. Однак, як засвідчують науковці, з точки зору артефактів і співпраці, пов'язаної з цифровими інноваціями, розуміння цифрової сумісності інформаційних систем потребує подальших наукових пошуків [62, с. 48; 63, с. 399].

Цифрова взаємодія або інтероперабельність виступає ключовою умовою для спільного створення цінності та кооперації в цифровому середовищі. У більш вузькому розумінні сумісність означає здатність двох або більше систем обмінюватися інформацією та ефективно її використовувати. Вона забезпечує можливість комунікації між системами через різні архітектурні рівні та організаційні межі, що є необхідною передумовою для комбінованої та розподіленої співпраці в рамках екосистем. Завдяки цьому сумісність сприяє численним перевагам, серед яких інтеграція характеристик програмних модулів та підвищена масштабованість [64].

Дослідники наголошують на потребі ширшого підходу до розуміння

цифрової сумісності, який виходить за межі суто технічного аспекту. Європейські науковці розглядають її в комплексному контексті, включаючи організаційні, правові та технічні складові, та звертають увагу на політичні чинники, що впливають на досягнення сумісності поза межами окремих організацій і держав. Особливу роль при цьому відіграє цифрова взаємодія як важлива організаційна здатність для ефективного управління розподіленими інформаційними системами та налагодження співпраці з партнерами у спільних або глобальних екосистемах [65, с. 419].

Американські дослідники К. Карху, Р. Густафссон і Б. Ітон визначають цифрові інновації через три ключові характеристики. По-перше, вони є комбінаторними, що означає здатність модульної багаторівневої архітектури дозволяти суб'єктам управління гнучко створювати нові комбінації шляхом інтеграції пристроїв, мереж, послуг та контенту. По-друге, цифрові інновації є мультिवаріантними, тобто передбачають участь численних, різноманітних та розосереджених суб'єктів, які охоплюють різні сфери суспільних відносин та галузі управління. По-третє, цифрові інновації акцентують увагу на цифрових технологічних платформах як центральних елементах інноваційної діяльності, що дозволяє розширювати базову функціональність інформаційних систем [66, с. 106-108]. Отже, за своєю суттю цифрові інновації – це соціотехнічний процес, в якому різні суб'єкти створюють нові продукти та послуги, поєднуючи та рекомбінуючи цифрові та фізичні компоненти.

Повертаючись до аналізу наукових досліджень щодо цифрової взаємодії суб'єктів публічного управління в умовах розвитку електронного урядування, варто відзначити Програму електронної комерції та цифрової економіки: підсумки 2022 року, затверджену на Конференції Організації Об'єднаних Націй з торгівлі та розвитку. У цьому документі підкреслюється необхідність посилення готовності до стрімкого розвитку цифрових технологій, а також їхній значний потенціал для забезпечення публічного управління у цифрову епоху на засадах прозорості, підзвітності та участі громадян [67].

Тож цілком очевидно, що електронне урядування може стати засобом для

досягнення цього. Тому саме запровадження цифрової взаємодії інформаційно-аналітичних систем органів публічної влади може забезпечити прозорість, підзвітність і участь, що лежить в основі електронного урядування. Завдання, які вирішуються при цьому, наступні: забезпечення діяльності уряду з орієнтацією на якісне задоволення потреб громадян при наданні адміністративних послуг; підвищення прозорості у діяльності завдяки оприлюдненні інформації в режимі реального часу; заохочення громадян до нових форм участі; удосконалення безпосереднього функціонування структурних підрозділів уряду через уніфіковане використання інформаційно-аналітичних систем на усіх рівнях публічного управління.

Німецький дослідник І.Ліпперт (Ingmar Lippert) зазначає, що у розвинених країнах сьогодні побудова двосторонніх каналів комунікації між громадянами та урядом у форматі C2G2C (громадянин-держава-громадянин) обумовлена стрімким розвитком цифрових технологій, зростанням використання Інтернету та розширенням можливостей електронного уряду. Така двонаправлена взаємодія значно спрощує інформаційні транзакції, які слугують платформою для зворотного зв'язку з громадянами та виступають одним із інструментів підзвітності уряду. Водночас, за словами науковця, дистанція між державними постачальниками послуг та громадянами може зменшитися завдяки наданню більшого доступу до осіб, що приймають рішення, через інтерактивні інформаційні системи та платформи, спрощуючи тим самим процес участі громадян у діяльності уряду [68].

Зокрема, сьогодні громадяни мають можливість генерувати онлайн-контент на деяких державних сайтах. Окрім збільшення кількості створених даних, категоризації та звітності про проблеми в спільноті чи територіальній громаді, вони також можуть організовувати онлайн-форуми щодо публічної політики, ініціатив та послуг. Як користувачі інформації, громадяни можуть більше брати участь у місцевих політичних процесах, посилювати комунікацію всередині громади, між громадою та урядом, створюючи більш інклюзивні та рівноправні канали комунікації.

Прикладами може бути створена у Великобританії платформа FixMyStreet, яка виступає як посередник між спільнотами та адміністраціями для розвитку діалогу, участі у місцевих справах та інформаційного обміну, а також платформи SeeClickFix у Канаді та США, які заохочують участь громади у наданні державних послуг [69; 70].

Ще одним прикладом може бути платформа Jaankari від уряду штату Біхар в Індії, яка включає кол-центр, спрямований на вирішення місцевих проблем та є зручним для громадян Біхару, оскільки економить їх час і гроші на поїздки в урядовий офіс і знижує шанси на несправедливе ставлення; крім того, це робить інформацію доступною для більш широкої аудиторії, включаючи ту категорію громадян, які є малописьменними, меншинами або громадянами з віддалених і слаборозвинених районів [71].

Як засвідчують відгуки громадян, ці інтерактивні відносини забезпечують коректну роботу уряду, обумовлюють чуйність до потреб і вимог громадян, а надання інформації в режимі реального часу підвищує прозорість уряду. Це значно знижує витрати на акумулювання, розповсюдження та доступ до урядових даних. Збір інформації покращується шляхом охоплення географічно, економічно та соціально розрізнених груп населення.

Крім того, Урядова інформація, така як бюджети, представлена за допомогою простих для розуміння візуальних інструментів. Також повідомляється, що цифрові платформи генерують «ефект відблисків», привертаючи увагу засобів масової інформації до оприлюднення причин, привертають увагу до поведінки уряду та збирають негайну реакцію громадян, щоб вказати на марнотратство, шахрайство чи зловживання.

Нові технології відкривають можливості для формування нових форм громадської участі. Децентралізація владних повноважень може здійснюватися через створення платформ для поширення інформації та взаємодії з нею. Колишній директор досліджень Інтернету та технологій Массачусетського технологічного інституту Л. Рейні (Lee Rainie) зазначає, що сучасні громадяни здатні самостійно обирати органи влади та джерела інформації, які вони

використовують, що сприяє демократизації знань, розширенню прав і можливостей особистості та підвищенню якості взаємодії між громадянами та урядом [72].

Вітчизняні науковці також підкреслюють значущість досліджень у сфері електронного урядування в умовах цифровізації. Зокрема, О. Скорик та Н. Рябоконт наголошують на потребі формалізації понятійно-категорійного апарату, удосконалення законодавчого регулювання, а також організаційно-технічного та кадрового забезпечення процесів розвитку електронного урядування і цифровізації [73]. К. Сімаков, В. Валіна, В. Лауніконіс, М. Будовій окреслюють ключові принципи цифровізації публічного управління в Україні, серед яких виділяють забезпечення рівних можливостей доступу до послуг, орієнтацію на міжнародне та міжрегіональне співробітництво, стандартизацію процесів надання послуг та впровадження комплексних національних цифрових стратегій. Науковці підкреслюють стратегічні пріоритети електронного урядування та цифрової трансформації економіки, наголошуючи, що розвиток вітчизняної цифрової економіки має передусім забезпечувати прогрес у суспільно значущих сферах: охороні здоров'я, освіті, екології, економіці та національній безпеці [74, с. 180]. Дослідники Г. Разумей, М. Разумей, проаналізувавши основні ініціативи 2019-2020 років Міністерства цифрової трансформації, зокрема функціонування додатків «ДІЯ», «Дія. Бізнес» та «Дія. Цифрова освіта», підкреслюють нагальну потребу у розвитку цифрових компетентностей публічних службовців та впровадженні цифрових і мобільних робочих місць [75, с. 140].

При цьому додамо, що нарощування цифрових знань та навичок публічних службовців має поєднуватися з розвитком цифрових компетентностей громадян, що забезпечить повноцінне використання новітніх цифрових можливостей та сприятиме підвищенню якості надання послуг і задоволеності потреб населення.

Вітчизняні дослідження проблем розвитку електронного урядування та цифровізації здійснюються і на рівні дисертаційних робіт. Так, Ю. Мохова у своїй докторській дисертації «Державні механізми розвитку електронного

урядування в умовах цифрових трансформацій України» (2021 р.) здійснила ґрунтовне теоретико-методичне обґрунтування та розробила науково-практичні рекомендації, спрямовані на вдосконалення державних механізмів розвитку електронного урядування. Ці заходи базуються на впровадженні цифрових технологій і мають забезпечити сталий розвиток України та ефективну реалізацію реформ [76].

С. Чернецький у дисертаційному дослідженні «Інформаційно-комунікативне забезпечення сталого демократичного врядування в Україні» (2023 р.) обґрунтовано необхідність розвитку концепції Відкритих даних як ключового інструменту підвищення ефективності роботи органів публічної влади та драйверу економічних можливостей. Автор доводить значущість їх розбудови для забезпечення прозорості діяльності публічних інституцій та підкреслює нагальну потребу у підвищенні цифрових навичок громадян України [77].

О. Романчук, у роботі «Електронне урядування: конституційно-правове дослідження» (2020р.) розглядає електронне урядування в Україні як безальтернативну трансформацію, що вже інтегрувалася в конституційно-правову реальність країни. Він зазначає, що електронне урядування слугує засобом розвитку та вдосконалення представницької демократії, створюючи нові ефективні механізми та можливості для участі громадян у вирішенні питань життєдіяльності відповідних територій [78, с. 9].

У дослідженнях, присвячених цифровій сумісності та взаємодії суб'єктів управління, можна виокремити принаймні дві основні концептуальні лінії. Перша — це роботи у сфері інформаційних технологій та комп'ютерних наук, які зосереджуються на технологічному аспекті сумісності, аналізуючи конкретні архітектурні рівні, елементи системи та стандарти її побудови. Друга — дослідження соціально-гуманітарного та управлінського спрямування, де цифрова сумісність розглядається не через технічні характеристики, а через наукове обґрунтування новацій у сфері управлінських процесів. Зокрема, такі дослідження фокусуються на алгоритмах управління, функціональних

повноваженнях персоналу в умовах цифровізації, нормативно-правовому забезпеченні, підвищенні цифрових компетентностей громадян, а також на інституційних механізмах, що сприяють або перешкоджають впровадженню певних технологій, стандартів чи платформ [79].

Проведений аналіз джерельної бази засвідчує наявність ґрунтовного масиву наукових розвідок, присвячених концептуальним засадам розвитку електронного урядування, а також трансформації управлінських процесів та модернізації сфери надання публічних послуг під впливом глобальної цифровізації. Попри значні здобутки у висвітленні загальних тенденцій електронного урядування, у вітчизняному науковому дискурсі спостерігається певний дефіцит комплексних досліджень, зосереджених саме на механізмах цифрової взаємодії органів публічної влади, в контексті інтеперабельності та координації. Відсутність цілісних методологічних напрацювань щодо налагодження ефективних каналів обміну даними та спільного використання цифрових платформ в умовах динамічного розвитку новітніх технологій об'єктивно актуалізує необхідність поглибленого наукового пошуку у досліджуваній сфері.

У першому розділі дослідження проаналізовано терміни і поняття «електронне урядування», «цифрова взаємодія органів публічної влади», «інформаційні системи». Наведено ключові підходи інформаційних платформ та міжнародних організацій до визначення поняття «електронне урядування». З'ясовано, що термін «електронне урядування» був вперше введений в 1993 році в Національному огляді ефективності США, термін «електронний уряд» набув поширення приблизно в 1997 році.

Встановлено, що визначення поняття цифрової взаємодії пов'язується із конкретним аспектом або сферою публічного управління. Обґрунтовано, що термін «цифрова взаємодія органів публічної влади» поки що не знайшов узгодженого наукового тлумачення, продовжує аналізуватись у наукових колах. Проведений аналіз дозволив виявити проблеми, що потребують здійснення

подальших наукових розвідок та дискусій, а також узгодження та законодавчого закріплення певних понять, зокрема, терміну «цифрова взаємодія органів публічної влади».

Систематизовано основні підходи до визначення поняття «інформаційні системи», «інтероперабельність», інших суміжних термінів. Обґрунтовано, що інформаційна система – це набір комп'ютеризованих компонентів, які використовуються для збору, створення та зберігання даних, які використовуються для обробки, аналізу та розповсюдження для прийняття управлінських рішень. Зазвичай він містить основні складові: апаратні компоненти, програмні компоненти, безпосередні дані, користувачі системи та процедури роботи даними. Доведено, що процеси інформаційного обміну є надзвичайно важливими, оскільки вони об'єднують цю систему як організовану сукупність елементів та інтегрують її можливості. Наголошено на потребі формування ефективних механізмів інтеграції комунікативних зусиль влади і суспільства у вирішенні спільних проблем.

Досліджено історичні витоки розвитку інформаційних систем, що становлять теоретичне підґрунтя формування державної політики у сфері цифрового розвитку та вдосконалення електронного урядування. Встановлено, що еволюція інформаційних систем охоплює останні шість десятиліть. Перший суттєвий етап розвитку пов'язаний із Другою світовою війною, коли промисловість багатьох країн трансформувалася в ефективну військову машину, що сприяло економічному зростанню та науково-технічному прогресу. Саме в цей період з'явилися перші комп'ютери (машини Т'юрінга), великі, малопотужні та незручні, але вони заклали основу для подальшого створення складніших інформаційних систем. Проаналізовано період впровадження World Wide Web у 1989 році, коли HTML-протокол започаткував нову еру технологічного розвитку та взаємодії систем. Доведено, що за останні шість десятиліть інформаційні системи перетворилися на фундамент будь-яких управлінських процесів, а принципи та алгоритми, закладені у 1960-1970-х роках, залишаються актуальними й сьогодні. Аналіз еволюційного розвитку інформаційних систем

XX сторіччя засвідчив, що 1960-1970-ті роки характеризуються організаційними мейнфреймами та міні-обчисленнями із спільним використанням даних; 1980-ті – розвитком персональних комп'ютерів без обміну даними; 1990-ті – розбудовою мереж із організаційними обчисленнями та обміном даними. Вивчено генезис розвитку інформаційних систем XXI століття та запропоновано періодизацію їх історичних етапів, що ілюструє трансформацію від інформаційного до цифрового суспільства.

Проаналізовано стан наукових досліджень щодо цифрової взаємодії суб'єктів публічного управління в умовах розвитку електронного урядування. Встановлено, що ця тема активно обговорюється як у зарубіжних наукових колах, так і вітчизняними дослідниками, охоплюючи як техніко-технологічні, так і соціо-гуманітарні аспекти. Обґрунтовано, що нові наукові дискурси виникають під впливом експоненційного зростання інноваційних платформ, ускладнення їх архітектури та стрімкого поширення в різних сферах управління. Проаналізовано здобутки зарубіжних і вітчизняних науковців у цій галузі.

Виявлено, що наукове поле цифрової сумісності та взаємодії суб'єктів управління формують дві концептуальні лінії: перша – техніко-технологічна, друга – соціо-гуманітарна, які взаємодоповнюють одна одну та поглиблюють науковий дискурс. Дослідження демонструють, що сучасні наукові розробки зосереджуються на кількох ключових напрямках: визначенні деструктивних чинників у розбудові інтероперабельності систем; розвитку новітніх цифрових платформ із відкритою архітектурою для забезпечення ефективного управління на принципах цифрової сумісності; дослідженні результатів функціонування таких систем та моделюванні їх майбутніх перспектив. Засвідчено необхідність подальших наукових пошуків у сфері цифрової сумісності та взаємодії органів публічної влади, а також вдосконалення їх інформаційних систем для підвищення ефективності публічного управління.

Основні результати дослідження, що викладені у першому розділі, висвітлено у таких публікаціях автора: [2; 45; 79].

## **РОЗДІЛ 2. ОСОБЛИВОСТІ МЕХАНІЗМІВ ЦИФРОВОЇ ВЗАЄМОДІЇ ТА ІНТЕРОПЕРАБЕЛЬНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ ТА СВІТІ**

### **2.1 Нормативно-правовий та організаційний механізми цифрової взаємодії органів публічної влади України в умовах розвитку електронного урядування**

Цифрова взаємодія органів публічної влади з населенням є невід’ємною складовою сучасного публічного управління. Її успіх значною мірою залежить від розвиненої законодавчої бази, оптимальної системи органів публічної влади на усіх рівнях управління, готовності суспільства прийняти нові технології тощо.

Першим нормативним актом у сфері інформаційної безпеки в Україні став Закон України «Про захист інформації в інформаційно-комунікативних системах» № 80/94-ВР (1994 р.) [80], який заклав правові засади захисту інформації в електронних системах, визначив обов’язки суб’єктів у сфері забезпечення безпеки інформаційних ресурсів та підкреслив значення конфіденційності, цілісності та доступності даних, що стало критично важливим у контексті стрімкого розвитку інформаційних технологій.

Наступним ключовим документом став Закон України «Про інформацію» від 6 липня 1999 року № 2657-IV [81], який визначає основні принципи інформаційної політики, встановлює порядок доступу до інформації та взаємодії між органами влади, створюючи основу для формування відкритого та цифрового суспільства. Цей закон заклав фундамент для подальшого розвитку правового поля, пов’язаного з електронними комунікаціями та доступом громадян до публічної інформації.

У 2003 році ухвалено Закон України «Про електронні документи та електронний документообіг» № 605-VII [82], який запровадив правові засади електронного документообігу, використання електронних підписів та печаток, що дозволило значно спростити та прискорити документообіг у публічному

секторі, підвищити ефективність роботи органів влади та забезпечити юридичну значущість електронних документів.

У 2010 році було прийнято Закон України «Про захист персональних даних» від 1 червня № 2297-VI [83], що закріпив правові механізми збору, обробки, зберігання та знищення персональних даних громадян, створивши надійні гарантії конфіденційності в цифровому середовищі та встановивши відповідальність за порушення правил обробки персональних даних.

Наступним важливим етапом стало ухвалення Закону України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI [84], який закріпив право громадян на отримання інформації, що знаходиться у володінні органів публічної влади та інших розпорядників публічної інформації, забезпечуючи прозорість та підзвітність їх роботи, що є одним із ключових принципів демократичного управління.

У 2015 році Президент України ухвалив Указ № 5/2015 «Про Стратегію сталого розвитку «Україна-2020»» [85], який визначив розвиток електронного урядування одним із пріоритетів реформування системи публічного управління, заклавши стратегічні орієнтири щодо цифровізації державних послуг і підвищення їхньої якості та доступності.

У 2016 році було затверджено Наказ Міністерства економічного розвитку і торгівлі та Міністерства регіонального розвитку, будівництва та ЖКГ України № 1501/248 від 8 вересня [86], який встановив порядок інтеграції інформаційних систем державних органів та органів місцевого самоврядування до Єдиного державного порталу адміністративних послуг, що дозволило централізувати надання електронних послуг, автоматизувати процеси міжвідомчої взаємодії та підвищити зручність доступу громадян і бізнесу до державних сервісів.

У 2017 році Кабінет Міністрів України ухвалив Розпорядження № 275-р від 3 квітня [88], яким затверджено середньостроковий план пріоритетних дій Уряду до 2020 року та план на 2017 рік, що закріпив розвиток електронного урядування як стратегічний пріоритет модернізації публічного управління та підвищення ефективності діяльності органів публічної влади.

Постанова КМУ № 627 від 16 червня 2021 року [88] визначає порядок обміну інформацією між органами, що контролюють справляння бюджетних надходжень, та органами місцевого самоврядування. Документ забезпечує стандартизований та своєчасний обмін даними, підвищує ефективність контролю за бюджетними надходженнями, сприяє автоматизації міжвідомчого обміну інформацією та підвищує якість фінансової звітності.

У вересні 2017 року було ухвалено Концепцію розвитку електронного урядування в Україні [89], головним завданням якої є створення ефективною, прозорою та доступною системи публічного управління за допомогою інформаційно-комунікативних технологій. Це включає забезпечення доступу громадян та юридичних осіб до державних послуг в електронному форматі, підвищення ефективності діяльності органів державної влади, а також сприяння відкритості та підзвітності влади перед громадськістю .

У 2018 році була ухвалена Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки та затверджено план заходів щодо її реалізації [90]. Документом окреслено ключові напрями цифрової трансформації адміністративних процесів у публічному управлінні. До цих напрямів віднесено: впровадження «цифрових» робочих місць, залучення громадян до етапів адміністративних процесів через соціальні мережі, прогнозування діяльності органів публічної влади на основі відкритих даних, використання технологій блокчейн та Інтернету речей, а також створення цифрових державних платформ. Визначено, що подальший цифровий розвиток суттєво вплине на здійснення адміністративних процесів в органах публічної влади. Метою концепції є підтримка та реалізація «Цифрової адженди України 2020», яка передбачає такі основні напрями: нормативне і організаційне забезпечення електронного документообігу, розвиток цифрової економіки, експорт цифрових технологій та підвищення цифрової компетентності суспільства.

В умовах стрімкого розвитку цифрових технологій та зростаючих кіберзагроз забезпечення кібербезпеки стало одним з ключових пріоритетів державної політики. У цьому контексті Закон України «Про основні засади

забезпечення кібербезпеки України», прийнятий у 2017 році [91], відіграє важливу роль у формуванні правової та організаційної бази для захисту життєво важливих інтересів людини, суспільства та держави в кіберпросторі. Закон визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також встановлює повноваження органів публічної влади і громадян, що є ключовими для забезпечення національної безпеки в умовах сучасних кіберзагроз.

План заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019-2020 роки [92] визначає пріоритетні напрямки розвитку електронної демократії, включаючи розвиток цифрових каналів комунікації між органами публічної влади та громадянами. Документом означено потребу в розробці та запровадженні нових законодавчих актів, зокрема щодо електронного голосування, референдумів та плебісцитів. Важливо, щоб створення та впровадження нормативних актів відбувалося у тісній співпраці між органами публічної влади та громадськими організаціями, що забезпечить відповідність законодавчих ініціатив сучасним вимогам та умовам.

План передбачає інтеграцію інструментів електронної демократії у різні сфери, такі як вищі навчальні заклади та веб-сайти органів виконавчої влади, що сприятиме підвищенню ефективності управлінських процесів і забезпечить рівний доступ громадян до інформації. Крім того, одним із завдань цього плану визначено потребу удосконалення нормативно-правової бази та функціональних можливостей Єдиного державного веб-порталу відкритих даних, що є ключовими для забезпечення прозорості та доступності інформації. Розширення інтеграції даних та стимулювання проєктів на базі відкритих даних допоможуть підвищити довіру до державних інститутів, а забезпечення ресурсної підтримки для розвитку інфраструктури електронної демократії є необхідним для її успішного впровадження та функціонування. Загалом, реалізація плану заходів сприятиме розвитку електронної демократії в Україні через інтеграцію сучасних технологій в управлінські процеси, забезпечення доступності інформації та підвищення рівня участі громадян [92].

Згідно з Постановою Кабінету Міністрів України від 30 січня 2020 року №56 «Деякі питання цифрового розвитку», були розроблені Методичні рекомендації, що регулюють реалізацію принципів державної політики цифрового розвитку органами виконавчої влади. Ці рекомендації визначають основні вимоги та принципи взаємодії органів виконавчої влади з державними та місцевими органами, громадянами і суб'єктами господарювання в рамках державної політики цифрового розвитку [93].

При цьому варто зазначити, що розвиток та впровадження цифрових технологій в Україні зумовили зростання попиту на стабільний і високошвидкісний Інтернет. У зв'язку з цим держава має підтримувати ефективні інвестиції та інновації постачальників електронних комунікативних мереж і послуг для розбудови інфраструктури та технологій, які забезпечать безперебійний зв'язок для всіх користувачів, незалежно від їхнього місцезнаходження чи типу кінцевого обладнання. Інвестиції в нові мережі та технології сприяють збільшенню вибору електронних комунікативних послуг та підвищенню їхньої якості.

Стратегія розвитку сфери електронних комунікацій України на період до 2030 року [94] передбачає подальший розвиток електронних комунікацій та інтеграцію сучасних технологій у всі аспекти публічного управління та суспільного життя, сприяючи побудові цифрового суспільства.

Систематизація нормативно-правових актів, що визначають концептуальні засади формування та розвитку механізмів цифрової взаємодії та інтероперабельності інформаційних систем органів публічної влади в Україні в умовах розвитку електронного урядування, наведена у таблиці, у якій відображено їх у хронологічній послідовності з урахуванням ключових положень і змістового наповнення (Додаток В).

Систематизація нормативно-правових актів у сфері цифрової взаємодії органів публічної влади дає підстави констатувати поступальний характер їх розвитку: від базових законів про інформацію та її захист до комплексних документів стратегічного спрямування. Виявленою закономірністю є

послідовний перехід від регламентації окремих процедур до формування інтегрованої нормативної екосистеми, яка охоплює електронне урядування, кібербезпеку, цифрову економіку та інструменти електронної демократії. Загальною тенденцією правового забезпечення є ускладнення та розширення його предмета під впливом внутрішніх реформаторських процесів та євроінтеграційних орієнтирів, що формує основу для подальшого вдосконалення системи електронного урядування.

Проте, незважаючи на значний прогрес у реалізації нормативно-правових механізмів досліджуваної проблеми, нами виокремлено прогалини в законодавчому забезпеченні, які гальмують подальшу розбудову цифрової взаємодії органів публічної влади та проявляються у:

– *недостатній інтеграції законодавчих актів*, оскільки існуючі закони часто не пов'язані між собою та мають різні підходи до регулювання одних і тих же аспектів цифрової взаємодії, що створює плутанину та ускладнює їх застосування. Стаття 2 Закону України «Про інформацію» визначає принципи інформаційної політики та доступу до інформації. Стаття 6 Закону України «Про державні інформаційні ресурси» встановлює правові засади створення, володіння, користування та розпорядження державними інформаційними ресурсами. Відсутність чіткої інтеграції між цими законами створює розбіжності в підходах до управління інформаційними ресурсами;

– *відсутності єдиного підходу до кібербезпеки* (незважаючи на ухвалення Закону України «Про основні засади забезпечення кібербезпеки України», не всі аспекти кібербезпеки чітко врегульовані). Стаття 1 визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки, при цьому спостерігається слабка деталізація питань щодо координації між різними органами публічної влади та чітких процедур реагування на кіберзагрози;

– *недосконалості правового регулювання електронного документообігу*. Закон України «Про електронні документи та електронний документообіг» не охоплює всі аспекти електронного документообігу, що створює правові прогалини та ускладнює його повсюдне впровадження;

– *недостатній регламентації прав і обов'язків користувачів електронних послуг*, що створює правову невизначеність та ускладнює захист прав громадян у сфері цифрової взаємодії. Стаття 6 Закону України «Про доступ до публічної інформації» закріплює право на доступ до публічної інформації, однак не визначає чіткої регламентації прав та обов'язків користувачів електронних послуг, зокрема у частині захисту персональних даних. Закон не повністю регулює процедури оскарження відмови в наданні інформації, що може створювати труднощі для громадян, які бажають захистити своє право на доступ до інформації. Що стосується Закону України «Про захист персональних даних», у ньому нема детальних положень про умови та процедури передачі персональних даних за кордон, що є важливим у контексті глобалізації та міжнародних транзакцій. Окрім того, як і у випадку з Законом України «Про доступ до публічної інформації», санкції за порушення вимог щодо захисту персональних даних є недостатніми, що знижує його ефективність у забезпеченні належного захисту даних;

– *обмеженому фінансуванню та технічному забезпеченню органів публічної влади*, що значно уповільнює впровадження нових технологій та модернізацію існуючих систем. Розпорядження Кабінету Міністрів України «Про затвердження середньострокового плану пріоритетних дій Уряду до 2020 року та плану пріоритетних дій Уряду на 2017 рік» містить невідповідність між визначеними пріоритетами та реальним фінансуванням цифрових ініціатив;

– *невідповідності стандартів*. Відсутність уніфікованих стандартів та вимог до інформаційних систем органів публічної влади призводить до їхньої несумісності та ускладнює інтеграцію цифрових рішень на національному рівні. Наказ Міністерства економічного розвитку і торгівлі України та Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України «Про затвердження Порядку інтеграції інформаційних систем державних органів та органів місцевого самоврядування до Єдиного державного порталу адміністративних послуг» регламентує лише загальні правила підключення систем до Єдиного державного порталу, проте не містить положень

щодо уніфікованих стандартів та вимог до інформаційних систем. Це зумовлює фрагментарність підходів і ускладнює інтеграцію цифрових рішень на національному рівні;

– *недостатній увазі до правових аспектів інноваційних технологій.*

Стаття 7 встановлює повноваження державних органів у сфері кібербезпеки, однак законодавство не завжди встигає адаптуватися до швидких змін у сфері цифрових технологій, зокрема у частині регулювання нових технологічних рішень, таких як блокчейн та штучний інтелект, що створює правові прогалини у регулюванні нових технологічних рішень.

Для подолання цих прогалин необхідно забезпечити комплексний підхід до вдосконалення законодавчої бази, що включатиме розробку єдиних стандартів, детальне регулювання ключових аспектів цифровізації, посилення координації між органами публічної влади та забезпечення належного фінансування цифрових ініціатив.

В контексті аналізу нормативно-правових механізмів цифрової взаємодії органів публічної влади України в умовах розвитку електронного урядування, видається доцільним звернутися також до міжнародних стандартів такої діяльності. Міжнародна організація по стандартизації (ISO) з моменту свого заснування приділяла значну увагу стандартизації різних аспектів роботи з документацією органів публічної влади. Стандарти ISO уніфікували багато процесів оформлення ділової кореспонденції. Незважаючи на те, що ISO наполягала на обов'язковому узгодженні та взаємодоповнюваності своїх стандартів, вони мали допоміжний характер і регламентували лише окремі аспекти роботи з цифровими документами. Проте, впровадження стандарту ISO 15489:2001 зробило значний внесок у розвиток управління цифровими документами [95]. Саме тому цей міжнародний стандарт був прийнятий майже у всіх розвинених країнах світу.

Міжнародний стандарт Міжнародної електротехнічної комісії (International Electrotechnical Commission, ІЕК) 82045-1:2001 «Управління документами. Частина 1: Принципи і методи» [96] розглядає управління

документами з точки зору виробничого процесу, надаючи чіткі рекомендації для поетапного управління документацією, що тісно інтегрується з етапами виробництва продукції. Цей стандарт регламентує управлінські процеси та детально визначає створення метаданих для документів, що є невід'ємною частиною сучасних управлінських практик. Запровадження ІЕК 82045-1:2001 стало важливим кроком у розвитку управління документами, завдяки чому забезпечено відповідність міжнародним стандартам та підвищено якість управлінських процесів.

Аналіз міжнародних стандартів ISO показує, що їх впровадження забезпечує значний прогрес у стандартизацію управлінських процесів. Проте, в Україні досвід застосування стандартів ISO в управлінні документами виявив певні проблеми. Зокрема, відзначено відсутність узгоджених дій при впровадженні цих стандартів, що веде до термінологічних та концептуальних суперечностей. Це ставить під сумнів ефективність прямого застосування міжнародних стандартів без належної адаптації до місцевих умов.

Українська система стандартизації, заснована на адаптації міжнародних стандартів ISO, стикається з низкою проблем, які гальмують її ефективне функціонування. Одним із ключових викликів є низький статус стандартів в Україні, що ускладнює їх впровадження на підприємствах та в органах публічної влади. Історично склалося так, що стандарти сприймалися як другорядний інструмент, а не як основа для підвищення якості продукції та послуг.

Крім того, процедури розробки та затвердження національних стандартів є надмірно бюрократизованими та тривалими. Обговорення проектів стандартів часто відбувається в обмеженому колі фахівців, що обмежує їхню релевантність та врахування інтересів усіх зацікавлених сторін.

Високі вимоги до кваліфікації фахівців у сфері стандартизації та відсутність належної фінансової підтримки ускладнюють залучення до цієї роботи досвідчених спеціалістів. Більшість розробок здійснюється на волонтерських засадах, що негативно впливає на якість та своєчасність виконання робіт.

Для вирішення зазначених проблем необхідно взяти комплексу заходів, спрямованих на:

- *підвищення статусу стандартів* (розробка та впровадження державної політики у сфері стандартизації, яка передбачає підвищення ролі стандартів у державному управлінні, економічному розвитку та соціальній сфері. Активізація інформаційно-просвітницької діяльності серед підприємств та громадськості щодо переваг стандартизації);

- *спрощення процедур стандартизації* (оптимізація процедур розробки, узгодження та затвердження національних стандартів, залучення до цього процесу зацікавлених сторін на всіх етапах. Широке використання інформаційних технологій для забезпечення прозорості та ефективності процедур стандартизації);

- *створення сприятливих умов для розвитку кадрового потенціалу* (забезпечення гідної оплати праці фахівців у сфері стандартизації, розробка програм підвищення кваліфікації та перепідготовки кадрів, створення кар'єрних траєкторій для молодих фахівців);

- *забезпечення фінансової стабільності системи стандартизації* (залучення додаткових фінансових ресурсів для розвитку системи стандартизації, зокрема, через механізми державно-приватного партнерства).

Впровадження зазначених заходів дозволить створити ефективну систему стандартизації, яка сприятиме підвищенню конкурентоспроможності української продукції на світових ринках, забезпеченню безпеки споживачів та захисту довкілля.

Розглядаючи організаційний механізм цифрової взаємодії органів публічної влади України, варто зазначити, що ефективність його функціонування цілком залежить від ефективності роботи структур, відповідальних за координацію та розвиток електронного урядування в Україні з урахуванням їхніх повноважень, функцій, взаємодії та впливу на загальний процес цифрової трансформації держави. Ця організаційна система охоплює Міністерство цифрової трансформації України (Мінцифри), а також відповідні

структури в центральних органах виконавчої влади (ЦОВВ), обласних державних адміністраціях (ОДА) та районних державних адміністраціях (РДА).

Мінцифри відіграє центральну роль, розробляючи та реалізуючи державну політику у сфері цифрової трансформації, інформаційного суспільства, електронного урядування, ІТ та електронних комунікацій. Воно координує діяльність інших органів виконавчої влади в питаннях цифровізації, розробляє та впроваджує нормативно-правові акти, стандарти та регламенти у сфері цифрової трансформації. Мінцифри також займається стратегічним плануванням та розробкою програм, інтеграцією та координацією між різними органами влади, освітніми ініціативами та забезпеченням кібербезпеки.

Центральні органи виконавчої влади (ЦОВВ), обласні державні адміністрації (ОДА) та районні державні адміністрації (РДА) відповідають за реалізацію політики цифрової трансформації на своїх рівнях. Вони розробляють та впроваджують електронні сервіси, координують процеси цифрової трансформації на регіональному та місцевому рівнях, надають електронні послуги громадянам.

Взаємодія між цими органами є ключовою для успішної цифрової трансформації. Мінцифри визначає загальні напрямки, ЦОВВ розробляють та впроваджують конкретні рішення, а ОДА та РДА забезпечують реалізацію на місцях. Однак, існують певні проблеми в координації, які можуть призводити до дублювання функцій, затримок у реалізації проектів та невідповідностей між рівнями управління.

Оцінюючи ефективність існуючої системи, можна виділити як позитивні результати, так і проблеми. З одного боку, впровадження порталу «Дія» та інших електронних сервісів значно спростило доступ громадян до державних послуг, зменшило корупцію та економить час і ресурси. З іншого боку, існують проблеми, такі як недостатнє фінансування, брак кваліфікованих кадрів, низький рівень цифрової грамотності та кібербезпекові ризики.

Кожен ЦОВВ, ОДА та РДА мають відповідні структури, що відповідають за реалізацію політики цифрової трансформації на своїх рівнях. Це включає

підрозділи, які займаються впровадженням електронних послуг, координацією цифрових проєктів, а також підтримкою та розвитком інформаційних систем.

Ці структури відіграють ключову роль у забезпеченні ефективної цифрової взаємодії, однак їхня діяльність також потребує координації та підтримки з боку центральних органів влади. Важливим аспектом є також забезпечення достатнього фінансування, професійної підготовки кадрів та підтримки на всіх рівнях управління для досягнення успішної цифрової трансформації.

Особливо важливою є проблема інформаційно-комунікативної взаємодії між владою та громадянами при вирішенні суспільно значущих питань. Громадяни часто отримують формальні відповіді, які сприймаються як відписки. Проте ситуація поступово покращується. Наразі на багатьох сайтах органів влади функціонують інтернет-приймальні для громадян, на численних порталах створені розділи «питання-відповідь» у режимі реального часу за допомогою чат-ботів, проводяться інтернет-опитування і голосування. Окрім цього, здійснюється моніторинг соціальних мереж, створюються офіційні акаунти і спільноти в соціальних мережах як від імені органів влади, так і окремих посадових осіб.

Однак існує проблема регламентації мережевої взаємодії з громадянами. З одного боку, публічні службовці часто не розуміють правил через недостатню інформацію про реальні плани своїх відомств і відсутність відповідальності за наслідки своїх дій. З іншого боку, структури мають велику свободу, що дозволяє їм ефективно взаємодіяти з громадянами. Це підкреслює необхідність термінового створення кодексу цифрового простору, який забезпечить комплексне регулювання цифровізації в Україні.

У процесі цифрової трансформації публічного управління, ключовим фактором є ефективність інформаційних систем, які використовують органи публічної влади.

Інформаційна система «Електронний уряд» призначена для збору, введення, пошуку, обробки, збереження та надання інформаційних ресурсів відповідно до визначених критеріїв на вимогу користувача. Вона спрямована на

надання органам публічної влади послуг фізичним та юридичним особам, а також на інформування про їх діяльність.

Дана інформаційна система регулюється такими нормативно-правовими актами: Постанова Кабінету Міністрів України «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» № 208 від 24.02.2003 р. [97]; Наказ Державного комітету зв'язку та інформатизації України «Про затвердження Переліку і Порядку надання інформаційних та інших послуг з використання електронної інформаційної системи «Електронний Уряд» № 149 від 15.08.2003 р. [98].

Основні цілі ІС «Електронний уряд» включають:

- забезпечення ефективних інформаційних комунікацій між органами публічної влади та формування централізованих баз даних із застосуванням технологій розподіленої обробки даних для підтримки електронного документообігу;
- надання органами публічної влади адміністративних послуг фізичним та юридичним особам у електронній формі, що гарантує доступність та зручність незалежно від часу і місця;
- стимулювання розвитку електронного ринку товарів та послуг, зокрема для забезпечення державних закупівель, організації тендерних процедур, а також підвищення ефективності управління виробництвом і реалізацією товарів і послуг, що, у свою чергу, підвищує конкурентоспроможність національних виробників на міжнародному ринку;
- впровадження механізмів електронної демократії, спрямованих на забезпечення прозорості діяльності органів публічної влади, зміцнення довіри між державою, громадянами, бізнесом та громадськими організаціями, а також надання можливості громадського контролю;
- підвищення якості життя громадян через удосконалення надання соціальних послуг, розвиток системи охорони здоров'я, забезпечення правової, екологічної та особистої безпеки, а також розширення освітніх можливостей;
- впровадження системи електронного голосування [99, с. 89].

На практичному рівні ІС «Електронний уряд» виступає інструментом реалізації всіх складових електронного урядування, включаючи надання адміністративних послуг фізичним та юридичним особам. Впровадження цієї системи забезпечує:

- підвищення достовірності, повноти та оперативності інформації, що використовується та накопичується в органах публічної влади;
- забезпечення прозорості виконання рішень і доручень органів публічної влади та високого рівня контролю за їх реалізацією;
- зниження накладних витрат у публічному секторі;
- зростання довіри суспільства до державних органів;
- ефективну взаємодію органів публічної влади з фізичними та юридичними особами, а також організацію зворотного зв'язку.

Інформаційна система «Звернення громадян» призначена для збору, введення, пошуку, обробки, збереження та надання інформаційних ресурсів відповідно до визначених критеріїв на запит користувача. Вона спрямована на оптимізацію обробки звернень громадян через автоматизацію процесів реєстрації, призначення виконавців та визначення строків виконання резолюцій.

Електронна версія системи, розроблена компанією Softline, забезпечує автоматизацію процесів реєстрації звернень, призначення виконавців та контролю за виконанням резолюцій. Це сприяє підвищенню оперативності управління діяльністю підрозділів, прискорює отримання статистичної та довідкової інформації про функціонування установи.

Інформаційно-аналітична система обліку звернень громадян «Звернення» доступна як у локальному, так і в мережевому варіантах. Мережевий варіант системи має додаткові можливості: одночасна робота необмеженої кількості користувачів; розмежування прав доступу користувачів до інформації та виконання дій; ведення обліку звернень у різних підрозділах; автоматичне надходження інформації про звернення до безпосередніх виконавців; персоналізація інтерфейсу системи для кожного користувача; автоматизація процесу створення резервних копій бази даних [100, с. 198].

Національний портал «Дія», який надає громадянам доступ до електронних державних послуг, інтегрує дані з багатьох інших державних реєстрів і систем, таких як реєстр фізичних осіб, державний реєстр юридичних осіб, реєстр транспортних засобів тощо. Інтеграція здійснюється через API та інші механізми обміну даними [101].

Єдиний державний реєстр судових рішень є інформаційною системою, яка забезпечує доступ до текстів судових рішень у відкритому доступі. Ця система інтегрована з іншими державними реєстрами та базами даних, що дозволяє автоматизувати процеси пошуку та обробки судових рішень. Інтеграція здійснюється через стандартизовані протоколи обміну даними [102].

Єдина інформаційна система соціальної сфери забезпечує управління соціальними послугами та виплатами, а також облік отримувачів соціальної допомоги. Ця система інтегрована з іншими реєстрами, такими як реєстр фізичних осіб та реєстр пенсійного фонду, що дозволяє автоматизувати процеси надання соціальної допомоги [103].

Згідно з Постановою Кабінету Міністрів України «Про порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» №3/2002 від 04.01.2002 р., наявність веб-сайту є основною вимогою для впровадження технологій електронного урядування. Органи публічної влади зобов'язані регулювати питання створення та функціонування веб-сайтів, зокрема, оперативно підготувати інформаційні матеріали, що мають загальнодержавне, регіональне або галузеве значення, та подати їх в електронному вигляді для оприлюднення на веб-сайтах [104].

Веб-сайти органів публічної влади повинні надавати населенню такі види інформаційних послуг:

- інформування: надання повної інформації про державні (адміністративні) послуги, включаючи їх найменування, адміністративний орган, нормативні документи, та консультаційні матеріали;
- одностороння взаємодія: розміщення електронних форм документів, необхідних для отримання послуг, з можливістю їх отримання, друку та

інструкціями щодо заповнення;

- двостороння взаємодія: прийняття заповнених електронних форм документів для надання послуг, включаючи ідентифікацію;
- здійснення трансакцій: реалізація можливостей прийняття рішень та їх доставка в електронній формі відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» №2155-VIII від 05.10.2017 р. [105].

Для ефективного надання інформаційних послуг через веб-сайти органи виконавчої влади створюють розділ «Каталог послуг». Цей розділ містить перелік державних (адміністративних) послуг, систематизованих за сферами їх надання – громадянам України, юридичним особам, державним службовцям, міжнародній спільноті. Послуги, що надаються в електронній формі, виділяються гіперпосиланнями на відповідні веб-сторінки

Аналіз функціонування офіційних веб-сайтів органів публічної влади засвідчив, що більшість із них здійснила перехід від початкового етапу «Розміщення інформації» до наступного етапу «Зворотний зв'язок». На цих веб-ресурсах представлено загальну інформацію про орган, його структуру, повноваження та нормативно-правову базу. Для організації зворотного зв'язку застосовуються різноманітні інструменти: електронні адреси, гостьові книги, поштові сервіси для зареєстрованих користувачів, електронні форми для подання звернень до посадових осіб за конкретними питаннями, а також розділи типу «Питання-відповіді», «Громадські приймальні», «Гарячі лінії». Додатково використовуються форуми для обговорення актуальних проблем і проведення соціологічних опитувань, що забезпечує інтерактивну взаємодію з громадянами.

Особливу увагу слід приділити Урядовому веб-порталу, який інтегрує веб-сайти майже усіх органів виконавчої влади та характеризується широкими інтерактивними можливостями. Він виступає центральним інтеграційним вузлом, що консолідує інформаційні ресурси та сервіси майже всіх міністерств і відомств у єдину екосистему. Такий підхід дозволяє реалізувати концепцію «єдиного вікна», де користувач отримує доступ до розгалуженої мережі інтерактивних можливостей без необхідності переходу між розрізненими

ресурсами. На порталі акумульовано важливі інструментарій: актуальні формуляри документів, супровід складних трансакцій, таких як реєстрація бізнесу «під ключ», ліцензування, отримання дозвільної документації, сертифікація товарів та автоматизована сплата податків.

Сучасний етап розвитку веб-сайтів органів публічної влади передбачає не лише дотримання міжнародних стандартів доступності та зручності інтерфейсів, а й гарантування захисту персональних даних громадян в умовах зростаючих цифрових загроз. Впровадження інтелектуальних чат-ботів дозволяє автоматизувати надання відповідей на типові запити, значно скорочуючи час очікування та знімаючи навантаження з операторів; використання технології розподіленого реєстру (Blockchain) стає гарантом незмінності інформації та виключає можливість корупційних маніпуляцій.

Ефективність функціонування веб-сайтів органів публічної влади та їх інформаційних систем залежить від здатності органів публічної влади оперативно реагувати на потреби громадян, забезпечувати зручний та безпечний доступ до послуг, впроваджувати інноваційні рішення та підтримувати актуальність і якість контенту. Лише таким чином можна досягти високого рівня задоволення громадян послугами, які надаються в електронній формі, та забезпечити ефективне функціонування системи електронного урядування в Україні.

Однак, вказані системи мають також і технологічні бар'єри. Основні з них включають недостатню уніфікацію даних між різними системами, що ускладнює інтеграцію, а також кібербезпекові ризики, що виникають при обміні даними між системами. Окрім того, існує обмежена автоматизація обробки текстових даних, що ускладнює аналітичні процеси та обробку великих обсягів інформації, оскільки існує низький рівень автоматизації обміну даними між різними відомствами, а також проблеми з уніфікацією даних та їхньою структурою.

Загалом, інформаційні системи органів публічної влади в Україні демонструють високу потенційну сумісність та здатність до інтеграції, однак, містять декілька ключових проблем. Використання різних технологічних

платформ і стандартів ускладнює інтеграцію систем, відсутність єдиних стандартів для структури та формату даних між різними системами, забезпечення безпеки даних під час їхньої передачі та зберігання є критично важливим і складним завданням, а недостатнє фінансування на модернізацію та підтримку інформаційних систем впливає на їхню здатність до інтеграції.

Серед технологічних бар'єрів, що уповільнюють ефективну взаємодію, можна виокремити використання у державних інформаційних системах застарілих технологій, що ускладнює їхню інтеграцію з сучасними платформами; відсутність цілісної стратегії цифровізації, що призводить до фрагментації зусиль та ресурсів, брак кваліфікованих ІТ-фахівців у державному секторі, що впливає на ефективність розробки та впровадження нових рішень; а також нестачу сучасної ІТ-інфраструктури, що включає обчислювальні потужності, мережеві ресурси та системи зберігання даних.

Вважаємо, що для їх подолання необхідне впровадження сучасних технологічних платформ і стандартів для забезпечення сумісності та інтеграції, розробку та впровадження єдиних стандартів для структури та формату даних, розробку та впровадження комплексних заходів для захисту даних, включаючи шифрування, багатофакторну аутентифікацію та регулярні аудити безпеки, підвищення кваліфікації існуючих ІТ-спеціалістів та залучення нових кадрів через освітні програми та тренінги, інвестиції в модернізацію ІТ-інфраструктури, включаючи розвиток хмарних рішень та підвищення пропускну здатності мереж.

Таким чином, зазначене дозволяє дійти висновку, що для підвищення ефективності роботи інформаційних систем органів публічної влади в Україні необхідно забезпечити їхню сумісність (інтероперабельність) та інтеграцію, а також подолати існуючі технологічні бар'єри, що вимагатиме комплексного підходу, а саме: модернізацію технологічної бази, уніфікацію даних, посилення кібербезпеки, інвестування в людські ресурси та розвиток ІТ-інфраструктури.

## **2.2. Характеристика механізмів цифрової взаємодії та інтеперабельності інформаційних систем органів публічної влади у провідних країнах світу**

Перетворення, що відбуваються на сучасному етапі суспільного розвитку, обумовлюють не лише підвищення ефективності і конкурентоспроможності органів публічної влади, а й переформатування відносин між державою і громадянином, що поступово поширюється й на віртуальну сферу. Однак варто зазначити, що вигода від потенціалу цифрової взаємодії та інтеперабельності інформаційних систем органів публічної влади не завжди очевидна, оскільки це багатовекторний процес переходу діяльності органів публічної влади у площину застосування цифрових технологій, що в контексті модернізації публічного сектора визначає завдання щодо вдосконалення організації управління органів публічної влади у напрямі повсюдної цифровізації.

Електронне урядування є способом організації публічної влади за допомогою систем локальних інформаційних мереж та сегментів глобальної інформаційної мережі, що забезпечує функціонування органів публічної влади в режимі реального часу та робить максимально простим і доступним щоденне спілкування з ними громадян, юридичних осіб, неурядових організацій тощо.

Отже, дані поняття співвідносяться як загальне до конкретного, тобто електронне урядування це частина цифровізації, оскільки останнє передбачає комплексний процес переходу до використання цифрових технологій.

Розвиток цифрових технологій стимулює створення нових кіберфізичних рішень та формування сучасних цифрових екосистем. Водночас ефективне використання потенціалу таких інновацій значною мірою залежить від цифрової сумісності як здатності двох або більше систем обмінюватися інформацією та правильно її інтерпретувати. Це особливо актуально в умовах, коли публічно-управлінські процеси трансформуються в електронний формат, а інформаційні системи та бази даних органів публічної влади повинні забезпечувати коректну взаємодію та обмін даними для підвищення ефективності управлінських

рішень [106].

Згідно з концепцією мережевого індивідуалізму Л.Рейні та Б.Велмана (Lee Rainie and Barry Wellman), цифрові технології «перевизначають» концепцію соціального капіталу, оскільки основні спільноти переходять від фізично фіксованих і обмежених груп до соціальних мереж завдяки цим новаціям. Такі новітні технології створили нові форми соціальної взаємодії, які неможливо виміряти за стандартними показниками соціального капіталу [107, с. 128].

Впровадження сучасних форматів публічного управління, орієнтованих на широке використання цифрових технологій, охоплює практично всі країни світу. Сучасні держави, враховуючи потреби та очікування громадян, активно трансформують системи надання послуг шляхом впровадження концепції цифрового уряду, що передбачає перепроєктування процесів із застосуванням інноваційних технологій та аналізу даних.

Цифрові технології та дані самі по собі не є трансформаційними чинниками. Лише системне інтегрування їх у процеси прийняття рішень, включно з розробкою комплексних стратегій і програм реформування публічного сектора, створює передумови для підвищення суспільного добробуту. Так, в Естонії запровадження електронного уряду дозволило громадянам здійснювати майже всі адміністративні процедури онлайн – від подання податкових декларацій до реєстрації підприємницької діяльності, що суттєво скоротило витрати часу та ресурсів на їх виконання.

Цифровізація докорінно змінила систему управління податками та зборами, бюджетну звітність, застосування цифрового підпису й ідентифікацію громадян, а також забезпечила перехід на єдину платформу надання державних електронних послуг. Такі нововведення зменшили адміністративне навантаження на підприємства та населення, підвищили швидкість, ефективність та зручність взаємодії з державними органами, одночасно скоротивши витрати. Наприклад, у Великобританії програма «Gov.uk Verify» через цифровий підпис дає можливість громадянам отримувати різні державні послуги [108].

Частка громадян, які користуються послугами електронного уряду (через

відвідування веб-сайтів органів публічної влади або безпосередню взаємодію з ними), останніми роками стабільно зростає, проте значно варіює між країнами. У Данії в 2016 році цей показник склав 88%, у Бразилії, Чилі, Італії, Мексиці та Колумбії він не перевищував 25%. Щодо онлайн-подачі заповнених форм, у Мексиці та Японії він становить менше 10%; у країнах Північної Європи, Естонії, Нідерландах і Франції цей показник перевищує 50% [109].

Ці відмінності зумовлені, зокрема, недостатньо розвиненою інфраструктурою, обмеженою пропозицією електронних послуг, а також структурними проблемами, пов'язаними з інституційними, культурними та економічними факторами.

Активна інтеграція електронних послуг в усі сфери суспільного життя простежується у Південній Кореї. Урядом вжито відповідні заходи, включно з електронним голосуванням та онлайн-освітою, що сприяло суттєвому підвищенню рівня цифрових навичок та активізації участі громадян у вирішенні питань місцевого значення. На противагу, наприклад у Мексиці, яка має нижчий рівень розвитку цифрової інфраструктури, доступ до Інтернету у віддалених регіонах значно ускладнений, що обмежує масштабування електронних послуг [110].

Таким чином, цифрова взаємодія суб'єктів публічного управління є складним, але необхідним процесом для підвищення ефективності надання адміністративних послуг, покращення загального добробуту суспільства. Вона вимагає не тільки технічного вдосконалення, але й комплексного підходу, через удосконалення законодавства, підвищення цифрової обізнаності населення та забезпечення рівних цифрових можливостей для всіх громадян.

Згідно з рейтингом ООН за рівнем розвитку електронного уряду (EGDI) Данія, Фінляндія, Республіка Корея, Нова Зеландія, Ісландія, Швеція, Австралія, Естонія, Нідерланди та Сполучені Штати лідирують у топ-10 за електронним урядуванням у 2022 році згідно з даними опитування ООН щодо електронного урядування [111]. Більшість цих країн впровадили стратегії цифровізації суспільства, активно використовуючи проривні технології, такі як блокчейн,

великі дані, штучний інтелект тощо.

Данія є яскравим прикладом успішного переходу до цифрового публічного управління. Було створено портал державних послуг [borger.dk](http://borger.dk), який надає персоніфіковану сторінку з доступом до конкретних послуг для кожного громадянина. Крім того, впроваджено обов'язкову цифрову поштову скриньку для фізичних осіб і підприємств, а також відкритий портал [sundhed.dk](http://sundhed.dk), що забезпечує доступ до персональних медичних даних. Ці цифрові сервіси значно полегшують громадянам доступ до державних послуг і інформації, підвищуючи ефективність взаємодії з публічними органами.

Для ефективної взаємодії з бізнесом у Данії функціонують ресурси [Virk.dk](http://Virk.dk) і [NemHandel](http://NemHandel). [Virk.dk](http://Virk.dk) є порталом для бізнесу, який надає доступ до різноманітних державних послуг і ресурсів, необхідних для ведення бізнесу. [NemHandel](http://NemHandel), у свою чергу, є відкритим середовищем електронного бізнесу, що дозволяє підприємствам безпечно та надійно відправляти стандартизовані електронні рахунки-фактури [112]. Ці сервіси сприяють підвищенню ефективності бізнес-процесів та зменшенню адміністративного навантаження на підприємства.

Завдяки реалізації Цифрової стратегії на 2016-2020 роки, яка визначила напрямки подальшої цифровізації державного сектору та його взаємодії з комерційними підприємствами й промисловістю, Данія успішно продовжує розвивати цифрове публічне управління та електронні сервіси. Одним із ключових пріоритетів стратегії стало створення платформи, що спрощує управління бізнесом та знижує адміністративне навантаження на підприємства. Зокрема, впровадження автоматизованої системи подання звітності дозволило досягти економії коштів у розмірі 3 млрд данських крон до 2020 року.

Також варто зазначити, що цифрові стратегії Данії включають надання компаніям доступу до більшої кількості даних державного сектора. Ці дані можуть стати основою для нових бізнес-можливостей та інновацій. Завдяки таким підходам Данія демонструє ефективну модель цифрового публічного управління, яка сприяє розвитку суспільства та економіки в цілому [112].

Багато країн приймають за взірець систему електронних закупівель

Південної Кореї ([www.g2b.go.kr](http://www.g2b.go.kr)) для розвитку своїх національних платформ. Ця система надає урядовим організаціям можливість здійснювати інтернет-аукціони в режимі реального часу, а також автоматизує всі етапи закупівельного процесу, включаючи подачу заявок, доставку та оплату, що значно підвищує ефективність і прозорість процедур. Крім того, в країні створено систему електронних закупівель KONEPS, яка забезпечує прозорість та ефективність у процесі державних закупівель. Ця система дозволяє електронним чином подавати тендерні пропозиції та укладати контракти, що значно зменшує корупцію та підвищує довіру до уряду [113].

Південна Корея також впровадила інші інноваційні рішення для підвищення ефективності публічного управління. Наприклад, система «Government 24» забезпечує громадянам доступ до понад 5,000 державних послуг через єдиний портал, що значно спрощує взаємодію з державними органами. Цей портал включає послуги, пов'язані з реєстрацією, сертифікацією, соціальними виплатами та багатьма іншими аспектами державного сервісу.

Ще один приклад – система G4C (Government for Citizens), яка об'єднує різні державні послуги в одному місці, надаючи громадянам зручний доступ до них через інтернет. Ця система дозволяє отримувати послуги без необхідності фізичної присутності в державних установах, що значно економить час та зусилля громадян.

Південна Корея також активно використовує технології штучного інтелекту для оптимізації державних послуг. Один із прикладів – проект «AI Citizen Assistant», який допомагає громадянам отримувати відповіді на запитання та доступ до необхідної інформації через чат-боти та голосові помічники.

Південна Корея також розвиває систему «Smart City», яка інтегрує різноманітні міські сервіси та інфраструктуру за допомогою IoT (Інтернету речей). Ця система дозволяє ефективніше управляти транспортом, енергопостачанням, безпекою та іншими аспектами міського життя, створюючи комфортні умови для мешканців [114].

Південна Корея активно впроваджує інновації у сфері електронного уряду.

Одним із яскравих прикладів є платформа для податкових послуг Hometax, яка дає можливість подавати податкові декларації та сплачувати податки онлайн. Це значно спрощує податкові процедури та підвищує їх прозорість.

У 2011 році було ухвалено План розвитку «розумного» електронного уряду, який забезпечив надання широкого спектра державних послуг через мобільні платформи. У межах цього плану створено портали, що надають громадянам доступ до митних, податкових, цивільних і патентних послуг, а також до онлайн-платформи e-People, яка дозволяє подавати цивільні звернення до адміністративних установ. Додатково функціонує система управління бізнес-процедурами уряду в режимі онлайн – On-nara [115].

Генеральний план електронного уряду, розроблений до 2020 року, передбачає трансформацію публічного управління на основі інтелектуальних інформаційних технологій. Ця трансформація спрямована на формування нової цифрової екосистеми, що слугуватиме платформою для урядових інновацій та забезпечить стійке економічне зростання. Серед ключових завдань плану визначено розвиток нових цифрових галузей, створення хмарної адміністративної інформаційної інфраструктури нового покоління та зміцнення позицій країни як провідного експорту технологій електронного уряду [115].

В Естонії одним із основних чинників розширення застосування цифрових державних послуг стало формування цифрової екосистеми на базі технології блокчейн, що реалізує концепцію «електронний уряд як послуга». Ця екосистема інтегрувала всі сфери публічної діяльності в єдиний інформаційний простір, створюючи безпечні платформи та уніфіковані дані, які використовуються як державним, так і приватним секторами. Розвиток цифрового суспільства в Естонії забезпечився завдяки децентралізованій інфраструктурі, підключеній до низки мереж, що гарантує гнучкість, відкритість і можливість впровадження нових функцій без потреби дорогих реконструкцій існуючих елементів [116].

Естонія належить до провідних країн світу у сфері електронного урядування та створила унікальну цифрову екосистему, яка включає такі інноваційні сервіси, як електронне резидентство, електронне голосування та

систему X-Road. X-Road є основною платформою естонської цифрової інфраструктури, забезпечуючи міжмережевий обмін даними між державними та приватними установами. Завдяки цій платформі громадяни можуть отримувати послуги швидко та безпечно, без необхідності повторного подання однакових даних у різні установи.

Програма електронного резидентства (e-Residency) дозволяє іноземним громадянам отримати цифровий ідентифікатор Естонії та керувати бізнесом у ЄС без фізичної присутності, що сприяло залученню іноземних інвестицій і створенню нових економічних можливостей. Крім того, Естонія стала першою країною, яка впровадила електронне голосування (i-Voting) на загальнодержавному рівні. Ця система дозволяє громадянам голосувати онлайн з будь-якої точки світу, що значно підвищує участь у виборах та робить процес більш зручним і доступним [117].

Базовою передумовою цифрової трансформації урядів є наявність початкового бюджетного фінансування, яке стимулює мобілізацію інвестицій з боку приватного бізнесу. У Великобританії цей процес реалізується через підтримку наукових досліджень і розробок у рамках публічно-приватного партнерства та державних закупівель. Однією з ключових ініціатив є платформа для високотехнологічного малого бізнесу - Digital Marketplace, що надає малим і середнім підприємствам можливість пропонувати свої товари та послуги державному сектору [118].

Ініціатива Small Business Research (SBRI) створює умови для презентації інноваційних рішень підприємцями та отримання фінансової підтримки для їх впровадження. Програма спрямована на вирішення конкретних суспільних викликів у сферах охорони здоров'я, екології та транспорту шляхом залучення малих підприємств до розробки сучасних технологій та послуг. Крім того, уряд активно підтримує інноваційні проекти через програму Innovate UK, що забезпечує фінансування для створення нових технологій і стимулює їх застосування в різних секторах економіки. Для забезпечення прозорості та ефективності публічних закупівель впроваджено портал Contracts Finder, який

дозволяє підприємствам знаходити та подавати заявки на державні контракти. Це сприяє залученню більшої кількості учасників до державних проєктів, забезпечуючи чесну конкуренцію та підвищуючи якість послуг. У рамках цифрової трансформації Великобританія також активно розвиває національну цифрову інфраструктуру, включно зі швидкісним інтернетом у всіх регіонах, що є критичною передумовою для ефективного функціонування цифрового уряду та економіки. Додатково уряд підтримує проєкти з кібербезпеки, спрямовані на захист державних і приватних даних, забезпечуючи безпечне надання цифрових послуг [118].

Сінгапур створив комплексну нормативно-правову базу для впровадження системи електронних закупівель уряду, що дозволило запустити портал GeBIZ. Цей портал надає постачальникам можливість шукати державні закупівлі, завантажувати тендерну документацію та подавати заявки в режимі реального часу. GeBIZ значно спростив процес участі в державних закупівлях, забезпечуючи прозорість і відкритість [119].

Крім системи електронних закупівель, Сінгапур активно розвиває інтегровані цифрові платформи для взаємодії різних органів влади та їх інформаційних систем. Одним із ключових компонентів цієї стратегії є проєкт Smart Nation, який передбачає створення інфраструктури для обміну даними між державними відомствами. Це дозволяє оптимізувати роботу урядових структур і забезпечує громадянам більш зручний доступ до державних послуг. Сінгапур також запровадив систему SingPass, яка є єдиною точкою входу для доступу до більш ніж 200 цифрових державних послуг. Завдяки SingPass громадяни можуть з легкістю взаємодіяти з різними державними установами, отримуючи доступ до послуг у сферах охорони здоров'я, освіти, податкової звітності та інших.

Уряд Сінгапуру активно використовує технології штучного інтелекту та великі дані для підвищення ефективності публічного управління. Наприклад, система Virtual Singapore створює тривимірну цифрову модель міста, яка допомагає планувати міське середовище, керувати транспортними потоками та розробляти стратегії реагування на надзвичайні ситуації [120]. Таким чином,

Сінгапур демонструє високий рівень цифрової взаємодії органів влади та їх інформаційних систем, забезпечуючи ефективність, прозорість і зручність державних послуг для громадян і бізнесу.

Цифрова взаємодія органів влади забезпечує нові підходи до створення прозорості та сприяння боротьбі з корупцією шляхом інтеграції залучення та участі громадян безпосередньо в ініціативи електронного уряду. Багато країн, що мають закони про прозорість, безпосередньо пов'язали імплементацію цих законів з реалізацією ініціатив, заснованих на повсюдній цифровізації. У Словаччині відкриті суди – ініціатива, яка сміливо рухається до цієї тенденції. Вона спрямована на покращення судової системи шляхом надання інформації про діяльність судів, а також аналізу даних для виявлення тенденцій та зв'язків, які в іншому випадку були б приховані, а також забезпечує комплексний механізм пошуку громадян для перевірки судів та суддів [121].

Аналіз світового досвіду свідчить, що цифровізація публічного управління є ефективним механізмом підвищення взаємодії між державними структурами та суспільством, а також зниження адміністративних та фінансових витрат. Так, перехід Данії на надання державних послуг виключно в цифровому форматі забезпечив значні економічні та організаційні вигоди: зокрема, знизив вартість окремих послуг на 50%. Запроваджена система зворотного зв'язку надала можливість взаємодії з усіма державними відомствами через персональний кабінет громадянина, а також здійснення бізнес-операцій у режимі онлайн, що дозволяє щорічно заощаджувати 10-20% державного бюджету.

У Великій Британії масштабна програма цифрової та технологічної оптимізації дозволила у 2016 році заощадити до 4,3 млрд доларів США завдяки впровадженню порталів державних послуг і систем електронного голосування, підвищенню контролю за державними закупівлями, оптимізації управління державною власністю через єдину систему автоматичної перевірки обґрунтованості витрат. У Саудівській Аравії використання великих даних у процесі цифровізації послуг з працевлаштування та спрощення бюрократичних процедур дозволяє економити до 1 млрд доларів щорічно. Згідно з Планом

побудови електронного уряду на 2016-2020 роки, вдосконалення онлайн-сервісів сприятиме скороченню часу та ресурсів, необхідних державним органам для обробки запитів громадян, щорічно знижуючи витрати приблизно на 500 тис. євро на країну, а для європейського бізнесу потенційна економія може становити від 4,4 до 50,4 млрд євро [122]. У Швеції Агентство соціального страхування розпочало програму цифровізації п'яти основних продуктів, які охоплювали 60% ручної обробки та понад 80% роботи кол-центрів агентства, що дозволило суттєво підвищити ефективність надання послуг [123].

Податкове управління Австралії використовує галузеві фінансові критерії, розроблені в результаті аналізу податкових декларацій більш ніж 1 млн малих і середніх підприємств, для виявлення фірм, які можуть занижувати доходи, і повідомляє їх про знайдені розбіжності [124]. Цифровізація допомоги на випадок хвороби в Норвегії дозволяє приймати рішення щодо покращення медичного обслуговування громадян та скорочення витрат [125].

Інновації в цифровому управлінні демонструють перспективи впровадження блокчейн-технологій. Деякі країни, такі як Дубай та Швеція, інтегрують блокчейн у сферу придбання нерухомості. У Дубаї планується запуск сервісів, що зв'язують Кадастрове управління з іншими державними установами, комерційними банками, розробниками та брокерами, створюючи «єдине вікно» для громадян і бізнесу [126].

У 2015 році уряд Фінляндії у співпраці з фінським стартапом MONI запустив експериментальні цифрові фінансові послуги, що дозволяють біженцям отримувати гроші і здійснювати платежі без відкриття банківського рахунку. Послуга використовує передплачену дебетову картку Mastercard, пов'язану з унікальною цифровою ідентифікацією на базі технології блокчейн. Податковий орган Великобританії використовує інструмент Connect для зв'язку понад 1 млрд елементів даних з 30 джерел, включаючи державні земельні та транспортні реєстри, сайти соціальних мереж і торгові асоціації, що допомагає виявляти можливі випадки ухилення від сплати податків [125].

Персоналізація державних послуг стає ключовим аспектом сучасного

публічного управління. Так, у Швеції батьки отримують регулярні електронні нагадування про заплановані медичні огляди та вакцинації для своїх дітей [127]. У Сінгапурі процес реєстрації компаній повністю оцифрований, що дозволяє скоротити більшість процедур до 15 хвилин із автоматичним повідомленням власника бізнесу про результати [128].

Розвиток компетенцій державних службовців виступає критичною передумовою ефективної цифрової трансформації публічного управління. Зокрема, в Академії урядової цифрової служби Великої Британії реалізується комплекс освітніх програм, спрямованих на підготовку фахівців цифрового сектора. Програма Digital, Data and Technology Profession передбачає формалізацію професійної спеціалізації в галузі цифрових технологій та даних для уряду, забезпечуючи можливість участі у реалізації значущих та комплексних цифрових проєктів [129].

Аналіз зарубіжного досвіду показує, що формування стратегії переходу до цифрового уряду, орієнтованого на громадян, є базовою умовою повної реалізації можливостей, які надає цифрова трансформація державного управління та суспільства в цілому. Це вимагає впровадження нових форм взаємодії, розвитку навичок і багатопланового використання великих масивів даних [130]. На основі аналізу механізмів цифрової взаємодії та інтеперабельності інформаційних систем органів публічної влади у провідних країнах світу, можна виділити декілька спільних аспектів, які є визначальними для розвитку електронного урядування та успішної цифровізації публічного управління.

1. Цілісна цифрова стратегія та політична воля. В усіх розглянутих країнах цифровізація є стратегічним пріоритетом, що підтримується на найвищому політичному рівні. Наприклад, у Данії, Естонії, Сінгапурі та Південній Кореї впроваджені цілісні цифрові стратегії, що охоплюють усі аспекти публічного управління та забезпечують узгодженість дій різних відомств і організацій.

2. Забезпечення інтеперабельності інформаційних систем.

Інтероперабельність, тобто здатність різних інформаційних систем взаємодіяти та обмінюватися даними, є ключовим фактором ефективності цифрового урядування. В Естонії, завдяки платформі X-Road, забезпечено обмін даними між різними державними та приватними установами, що сприяє швидкому та безпечному наданню послуг громадянам.

3. Розвинена цифрова інфраструктура, яка є основою для функціонування електронного уряду. У Великобританії, Данії та Південній Кореї активно впроваджуються високошвидкісні інтернет-з'єднання, що забезпечують доступ до цифрових послуг навіть у віддалених районах.

4. Єдині портали для надання державних послуг. Більшість розглянутих країн впровадили єдині портали для надання державних послуг, що значно спрощує взаємодію громадян з органами влади. Наприклад, у Данії портал borger.dk, у Південній Кореї портал Government 24, у Сінгапурі система SingPass забезпечують зручний доступ до численних послуг через один інтерфейс.

5. Прозорість та боротьба з корупцією. Цифровізація сприяє підвищенню прозорості публічного управління та зменшенню рівня корупції. Системи електронних закупівель, такі як GeBIZ у Сінгапурі та KONEPS у Південній Кореї, забезпечують прозорість процедур і підвищують довіру до уряду.

6. Забезпечення безпеки та конфіденційності даних є критично важливим аспектом цифрового урядування. В Естонії технологія блокчейн використовується для захисту даних, а у Великобританії уряд активно підтримує проекти з кібербезпеки.

7. Підтримка інновацій та залучення приватного сектора. У Великобританії ініціативи як Innovate UK та Small Business Research (SBRI) сприяють розвитку нових технологій і стимулюють їх впровадження у різних секторах економіки.

8. Підвищення цифрової обізнаності населення. Розвиток цифрових навичок серед населення є необхідним для успішного впровадження

електронних адміністративних послуг. Південна Корея та Сінгапур активно працюють над підвищенням рівня цифрової грамотності громадян, забезпечуючи їм доступ до освіти та тренінгів.

Підсумовуючи, зазначимо, що успішний розвиток електронного урядування вимагає комплексного підходу, що включає розробку цілісних стратегій, забезпечення інтегрованості інформаційних систем, розвиток цифрової інфраструктури, створення єдиних порталів для надання послуг, забезпечення прозорості та безпеки, підтримку інновацій та підвищення цифрової грамотності населення. Ці аспекти є спільними для провідних країн світу, які успішно впроваджують цифрові технології у публічне управління, підвищуючи ефективність адміністративних послуг та сприяючи загальному добробуту суспільства.

### **2.3 Безпекові виклики та можливості цифрової взаємодії органів публічної влади в Україні**

Технологічний прогрес значно посилює необхідність забезпечення високого рівня безпеки у публічному просторі. Інновації зарекомендували себе як безперервний процес в публічних установах, що використовує потенціал висококваліфікованих службовців. Використання додатків, доповнень і інтелектуальної автоматизації процесів значно зменшує прогалини у цифровізації, що забезпечує відповідний рівень безпеки. Спільне використання сенсорних технологій інтернету речей (IoT), автоматизований моніторинг цифрового простору та цифрові ланцюги проведених на блокчейн транзакцій та дій забезпечують максимальну безпеку в публічному просторі та захист у кібернетичному контексті.

Перехід до системи «єдиного вікна» з доступом до найновіших даних та інформації через ергономічний портал, створення спільних міжвідомчих платформ обумовлює потребу у розробці гнучких і високочутливих модулів для забезпечення кількісно оцінених ризиків впровадження. При цьому важливим

аспектом є прозорість платформи, яка дозволяє користувачам бачити, хто використовує їхні дані, з якою метою та як вони захищені.

Регулярне висвітлення у засобах масової інформації випадків кібератак на органи публічної влади негативно впливає на рівень суспільної довіри до захисту персональних і службових даних. У зв'язку з цим актуальним є впровадження комплексних підходів до забезпечення кібербезпеки, які охоплюють державні інформаційні системи, бізнес-середовище та громадян, формуючи цілісну й узгоджену модель захисту цифрової інфраструктури. Суб'єкти публічного управління, що надають державні електронні послуги, повинні стати першими ініціаторами кібербезпеки, регулярно проводячи аудити та виявляючи технологічні вразливості. Важливою також є прозорість у використанні даних, яка створює необхідну довіру до платформи та влади [131]. При цьому системи керування контентом повинні пропонувати безбар'єрний багатоканальний доступ, підготовлений з урахуванням мов і культур. Активна участь громадян повинна підтримуватись за допомогою гейміфікації, що сприяє підвищенню обізнаності щодо безпеки та заходів профілактики [132].

Для забезпечення максимальної безпеки та ефективності роботи органи публічної влади повинні крок за кроком впроваджувати інновації та новітні технології. Послідовне впровадження цифрових рішень дозволять досягти значного прогресу у підвищенні рівня безпеки та ефективності публічного управління.

Згідно з дослідженнями 2022 року значна кількість європейських держав здійснила комплексну цифрову трансформацію систем публічного управління [133]. Провідні позиції у цьому процесі посідають країни Північної Європи, зокрема Фінляндія, Данія та Швеція; до групи держав із високим рівнем цифровізації також належать Естонія та Мальта. У сучасному західному суспільстві цифрові технології стали невід'ємним елементом повсякденного функціонування громадян і бізнесу, охоплюючи використання мобільних пристроїв, мережі Інтернет, електронної ідентифікації, програмних застосунків та інструментів безготівкових розрахунків. Це створює потребу в органах влади

німецькомовних країн більше зосередитися на орієнтації на клієнта та впровадженні ефективних рішень для використання синергії цифровізації. Зростання кількості хакерських атак та витоків даних із інформаційних систем органів публічної влади підвищує відчуття небезпеки серед громадян.

Цифровізація процесів у публічному управлінні певною мірою поки що обмежується переведенням паперових документів у електронні формати. Хоча такі заходи формують необхідне технічне й організаційне підґрунтя для подальших трансформаційних змін, самі по собі вони не забезпечують суттєвого підвищення ефективності управлінських процесів. Водночас фрагментарне впровадження різномірних центрів обробки даних і програмних рішень зумовлює неузгодженість цифрової інфраструктури, що ускладнює взаємодію органів публічної влади з отримувачами адміністративних послуг.

Вищезазначене доводить, що цифрова взаємодія перетворилася на невід'ємний елемент функціонування органів публічної влади, що актуалізує потребу у забезпеченні належного рівня інформаційної та кібернетичної безпеки. Інтеграція сучасних технологічних рішень у їх діяльність сприяє підвищенню результативності та прозорості надання державних послуг, розширює можливості доступу громадян до публічної інформації та забезпечує оперативніше реагування на суспільні запити. Водночас поряд із новими можливостями цифрова взаємодія в системі органів публічної влади України супроводжується комплексом суттєвих безпекових ризиків і викликів, що потребують системного управлінського реагування.

Вважаємо, що до таких викликів варто віднести: недостатню деталізацію положень у законодавстві з кібербезпеки; відсутність конкретних стандартів і вимог до кібербезпеки для різних сфер публічного управління; недостатню координацію діяльності між органами публічної влади, особливо у горизонтальній площині; обмежене фінансування та ресурси; невідповідність міжнародним стандартам та найкращим практикам у сфері кібербезпеки; нестача кадрів та освітніх програм тощо.

*Недостатня деталізація положень у законодавстві з кібербезпеки*

становить суттєву перешкоду для їх практичної реалізації та ефективного правозастосування. Нормативно-правові акти нерідко обмежуються декларативними положеннями без належної процедурної деталізації, що зумовлює неоднозначність тлумачення та ускладнює їх імплементацію. Зокрема, відсутність уніфікованих критеріїв і формалізованих процедур оцінювання кіберзагроз та реагування на кіберінциденти створює значні організаційні та управлінські труднощі як для органів публічної влади, так і для суб'єктів приватного сектору. Так, Закон України «Про кібербезпеку» визначає загальні засади функціонування національної системи кібербезпеки, однак не містить чітко регламентованих алгоритмів дій у разі виникнення кіберінцидентів. Закон України «Про захист інформації в інформаційно-комунікаційних системах» [80], встановлюючи базові вимоги до інформаційної безпеки, не передбачає конкретних методик та індикаторів оцінювання рівня захищеності інформаційних систем. Така нормативна невизначеність зумовлює фрагментарність підходів до забезпечення кібербезпеки в різних організаціях та ускладнює міжвідомчу координацію і взаємодію.

У цьому зв'язку доцільним видається розроблення та системне впровадження уніфікованих національних стандартів у сфері інформаційної безпеки, зокрема ДСТУ ISO/IEC 27001:2017 «Системи управління інформаційною безпекою», які здатні забезпечити формування чітких, формалізованих критеріїв і процедур оцінювання кіберзагроз та рівня захищеності інформаційних систем.

Однак варто також зазначити, що у 2020 році ухвалено Закон України «Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації» [134], який запровадив поняття комплексної системи захисту інформації. Попри це, нормативні положення залишаються недостатньо деталізованими з огляду на відсутність чітко визначених критеріїв оцінювання відповідності інформаційних систем встановленим вимогам. Зокрема, на рівні законодавчого регулювання не повною

мірою визначено порядок організації та проведення державної експертизи, перелік індикаторів і процедур оцінювання, а також коло уповноважених суб'єктів, відповідальних за її здійснення. Додаткові питання виникають у зв'язку з передбаченою можливістю оброблення окремих категорій інформації без повноцінної комплексної системи захисту, оскільки вимоги до таких інформаційних систем залишаються недостатньо конкретизованими. У сукупності це зумовлює необхідність подальшого нормативного уточнення стандартів, методик та процедур оцінювання у сфері інформаційної безпеки.

Окрім того, імплементація нових нормативних вимог потребує значних часових і ресурсних витрат, що зумовлює необхідність розроблення відповідних підзаконних актів, а також проведення системної інформаційно-роз'яснювальної роботи серед органів публічної влади та суб'єктів господарювання.

Проблемним залишається й те, що чинні нормативно-правові акти не завжди містять достатньо деталізовані процедури реагування на кіберінциденти. Так, постанова Кабінету Міністрів України від 23 грудня 2020 року № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» закладає інституційні та організаційні засади функціонування відповідної національної системи, визначає Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України відповідальним суб'єктом, передбачає технічне оснащення об'єктів критичної інфраструктури засобами збору даних про кіберзагрози, а також окреслює механізми міжвідомчої взаємодії у сфері кібербезпеки [135]. Це свідчить про формування системного та централізованого підходу до управління кіберзахистом із визначенням інституційної відповідальності. Разом із тим постанова характеризується недостатнім рівнем процедурної конкретизації реагування на кіберінциденти, а також відсутністю чітко сформульованих критеріїв оцінювання результативності функціонування відповідної системи.

Постанова КМУ «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 4 квітня 2023 року № 299

логічно розширює попередні нормативні підходи, деталізуючи процедурні аспекти реагування на кіберінциденти. Документ визначає послідовність ключових етапів реагування — від виявлення та аналізу інциденту до його локалізації, усунення наслідків і відновлення функціонування систем; запроваджує класифікацію кіберінцидентів за рівнем критичності; а також передбачає розроблення методичних рекомендацій для суб'єктів системи кібербезпеки з метою уніфікації практик реагування. Разом із тим дискусійними залишаються питання практичної імплементації таких рекомендацій, зокрема механізми моніторингу їх виконання, а також недостатня визначеність інструментів відповідальності за порушення встановлених вимог.

Отже, зазначені нормативні акти формують важливий етап інституціоналізації національної системи кібербезпеки, закладаючи нормативно-правові засади для підвищення спроможності органів публічної влади до ефективного реагування на кіберінциденти в інформаційно-комунікаційних системах [136].

У цьому зв'язку видається доцільним подальше узгодження національного законодавства з міжнародними підходами, зокрема шляхом орієнтації на стандарти серії ISO/IEC 27035, розроблені Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Зазначені стандарти визначають структуровані підходи до управління інцидентами інформаційної та кібербезпеки, охоплюючи процеси їх виявлення, аналізу, реагування та відновлення функціонування систем після порушень безпеки. Їх міжнародне визнання зумовлює високу практичну релевантність та можливість використання як методологічної основи для вдосконалення національної нормативної бази.

Усуваючи ці прогалини, Україна зможе подолати виявлені нормативні прогалини шляхом деталізації процедур і запровадження уніфікованих стандартів, що сприятиме формуванню більш цілісної та стійкої системи кібербезпеки. Це, своєю чергою, забезпечить чітке визначення функцій і відповідальності суб'єктів, підвищить рівень міжвідомчої координації та

ефективність реагування на сучасні кіберзагрози.

Наступним безпековим викликом цифрової взаємодії органів публічної влади вважаємо *відсутність конкретних стандартів і вимог до кібербезпеки для різних сфер публічного управління*, зокрема об'єктів критичної інфраструктури. Цифрова трансформація органів публічної влади створює нові ризики у кіберпросторі, особливо коли мова йде про критично важливі об'єкти, які забезпечують безперервне функціонування суспільства: енергетику, транспорт, зв'язок, охорону здоров'я та інші. У розвинених країнах правове регулювання та ініціативи щодо захисту критичної інфраструктури вже впроваджено. Наприклад, у Європейському Союзі ключовими інструментами є Директива NIS-2 та Директива CER. Важливість директиви NIS-2 відзначається комплексним підходом, що охоплює як технічні, так і організаційні та нормативні аспекти мережевої та інформаційної безпеки. Вона встановлює суворіші вимоги та чіткі стандарти захисту критичної інфраструктури та цифрових послуг, розширює перелік секторів, що вважаються критичними, та посилює транскордонне співробітництво між країнами-членами ЄС [137]. Директива CER спрямована на підвищення стійкості критичної інфраструктури до різних загроз, передбачає запровадження державами-членами заходів для посилення фізичної та операційної безпеки критичних об'єктів, визначення критичної інфраструктури у різних секторах, регулярну оцінку ризиків та загроз, а також розробку стратегій управління надзвичайними ситуаціями та кризами [138]. Таким чином, міжнародний досвід демонструє важливість формалізації стандартів кібербезпеки та розробки комплексних підходів до захисту критично важливих секторів державного управління.

Особливе значення критичної інфраструктури визначається кількома ключовими факторами: її системною важливістю, високою взаємозалежністю та привабливістю для кіберзлочинців. Такі об'єкти забезпечують життєво необхідні послуги, від функціонування яких залежить стабільність суспільства. Порушення роботи навіть одного елемента критичної інфраструктури може спричинити каскадні ефекти, паралізуючи цілі економічні сектори. Через свою

значущість ці об'єкти стають привабливою мішенню для кібератак, а відсутність чітких стандартів кібербезпеки підвищує ризик появи вразливостей, які можуть бути використані зловмисниками. Кібератаки на критичну інфраструктуру призводять до економічних збитків через збої у роботі підприємств, втрату даних та шкоду репутації, а також можуть слугувати інструментом гібридної війни, створюючи геополітичні ризики.

Для подолання цих викликів необхідно розробити та впровадити національні стандарти кібербезпеки, що враховують специфіку різних секторів публічного управління. Усі об'єкти критичної інфраструктури повинні проходити сертифікацію на відповідність встановленим вимогам цих стандартів, що забезпечить комплексний і системний захист від потенційних загроз.

*Недостатня координація між державними органами є ще одним суттєвим безпековим викликом та визначальною проблемою у сфері кібербезпеки.* Відсутність ефективних механізмів взаємодії та спільної роботи між різними органами, відповідальними за забезпечення кіберзахисту, ускладнює обмін інформацією та координацію дій під час реагування на кіберінциденти. Така фрагментація зусиль призводить до того, що навіть за наявності окремих ініціатив із посилення кібербезпеки загальний рівень захисту залишається недостатнім через відсутність скоординованого підходу та інтегрованого використання ресурсів.

В Україні створено кілька структур, відповідальних за забезпечення кібербезпеки, проте дискусійним залишається питання щодо ефективності їхньої діяльності та можливості формування єдиного потужного центру кіберзахисту, який об'єднав би зусилля всіх суб'єктів у цій сфері.

Як зазначалось вище, одним із ключових суб'єктів у сфері кібербезпеки є Державний центр кіберзахисту при Державному агентстві спеціального зв'язку та захисту інформації, який виконує важливі функції щодо підвищення рівня захисту державних інформаційних ресурсів [139; 140]. Незважаючи на наявність цього центру, загальна ситуація у сфері кібербезпеки в Україні залишається складною та потребує системного врегулювання.

Національний координаційний центр кібербезпеки, який функціонує як робочий орган Ради національної безпеки і оборони України, відповідає за координацію дій різних державних органів у сфері кіберзахисту. Проте його діяльність часто критикують через обмежене фінансування та недостатні повноваження. Державне підприємство «Галузевий центр кібербезпеки» зосереджується на забезпеченні безпеки у критичних інфраструктурних секторах [141].

Існує декілька ключових проблем, що перешкоджають ефективній роботі у сфері кібербезпеки, можна виділити: розподілену відповідальність між різними органами публічної влади, що ускладнює координацію їхніх дій; недостатнє фінансування, яке не дозволяє реалізувати ефективні заходи захисту; дефіцит висококваліфікованих фахівців у сфері кібербезпеки; відсутність єдиної стратегії, що чітко визначала б національні пріоритети та цілі у сфері кіберзахисту. Ці фактори у сукупності знижують ефективність існуючих механізмів та створюють потенційні ризики для безпеки державних інформаційних систем.

Незважаючи на існування окремих структур, які займаються питаннями кібербезпеки в Україні, їхня ефективність потребує значного покращення. Для створення ефективної системи кіберзахисту необхідно вирішити проблеми координації, фінансування та кадрового забезпечення, що дозволить підвищити надійність захисту критичної інфраструктури та загальний рівень кібербезпеки в країні.

На нашу думку, вирішення цих проблем передбачає комплекс заходів: створення єдиної системи координації кібербезпеки, яка б об'єднувала зусилля на всіх рівнях управління та мала розширені повноваження для оперативного прийняття рішень; збільшення фінансування заходів з кібербезпеки, що дозволить реалізувати сучасні технологічні рішення та підтримувати постійний розвиток систем захисту; розробка довгострокової стратегії кібербезпеки, яка визначатиме пріоритети та цілі на найближчі роки і слугуватиме орієнтиром для державних органів та приватного сектору; підвищення рівня обізнаності

населення, зокрема через інформаційно-освітні кампанії, що сприятиме формуванню культури кібербезпеки серед громадян; активне залучення приватного сектору до розробки та впровадження заходів кіберзахисту, з використанням потенціалу технологічних компаній та консалтингових структур; інтеграція Державного центру кіберзахисту Держспецзв'язку у єдину систему координації, наділення його розширеними повноваженнями та об'єднання існуючих структур у рамках централізованого управління кібербезпекою, що стане ключовим кроком для підвищення її рівня в Україні. Ці заходи у сукупності дозволять сформувати більш скоординовану, ресурсно забезпечену та технологічно оснащену систему кіберзахисту, здатну ефективно протидіяти сучасним загрозам.

Органи публічної влади, що надають електронні державні послуги, є особливо привабливою мішенню для кібератак через великі обсяги персональних даних, фінансову інформацію та критичну інфраструктуру. Як ефективний інструмент для вирішення цієї проблеми ми пропонуємо застосовувати розроблену нами Індикативну панель відстеження кіберзагроз. Вона забезпечує систематизацію процесів відстеження та аналізу потенційних загроз, дозволяючи створити централізовану структуру для відстеження кіберризиків. За допомогою цього інструменту органи публічної влади можуть виявляти слабкі місця в системах захисту, оперативно реагувати на інциденти та впроваджувати превентивні заходи, спрямовані на мінімізацію ризиків. Пропонована панель (таблиця 2.1) складається з наступних показників:

- *показник* ■ конкретний параметр, який відстежується (наприклад, кількість невдалих спроб входу, обсяг аномального трафіку тощо);
- *частота моніторингу* ■ щогодинно, щомісяця, щотижня, щодня;
- *метод моніторингу* - спосіб відбору даних про цей показник (логі файли, SIEM-система, ручний аналіз тощо);
- *відповідальний* за моніторинг цього показника;
- *поріг тривоги* - значення показника вважається критичним і вимагає негайної реакції; наприклад, якщо середньодобова кількість невдалих спроб

входу в систему становить 100, то це вважається нормою.

Перевищення на 50%, 30% означає, що якщо кількість невдалих спроб входу перевищить 150 (100 + 50% від 100) або 130 (100 + 30% від 100) за добу, то це вже вважається аномалією і сигналізує про можливу атаку. Для різних показників можуть встановлюватися різні пороги тривоги. Наприклад, для обсягу мережевого трафіку поріг може бути вищим, оскільки його коливання можуть бути більш значними. Поріг тривоги також залежить від того, наскільки критичним є цей показник для системи. Для критичних систем поріг тривоги може бути встановлений нижче, щоб швидше реагувати на будь-які відхилення від норми. Якщо середній обсяг аномального трафіку до сервісів електронних послуг становить 10 Гб на добу, а поріг тривоги встановлений на рівні перевищення середнього на 30%, то будь-який обсяг аномального трафіку, що перевищує 13 Гб (10 Гб + 30% від 10 Гб), буде вважатися підозрілим і вимагатиме додаткової перевірки;

– дії при перевищенні порогу - які дії необхідно вжити, якщо значення показника перевищує поріг тривоги.

Таблиця 2.1

Індикативна панель відстеження кіберзагроз у органі публічної влади

Показник	Частота відстеження	Метод відстеження	Відповідальний	Поріг тривоги	Дії при перевищенні порогу
Кількість невдалих спроб авторизації	Що-годинно	SIEM, лог-файли шлюзів	Адміністратор безпеки	Перевищення середнього на 50%	Блокування IP, аналіз логів, посилення аутентифікації
Обсяг аномального трафіку до сервісів електронних послуг	Що-годинно	SIEM, IDS/IPS	Адміністратор мережі	Перевищення середнього на 30%	Блокування трафіку, аналіз логів, перевірка на шкідливе програмне забезпечення
Кількість виявлених вразливостей в системі	Що-денно	Сканування вразливостей	Адміністратор безпеки	Нові критичні вразливості	Усунення вразливостей, оновлення ПО

## Продовження таблиці 2.1

Зміни конфігурації серверів електронних послуг	Що-годинно	SIEM, інструменти конфігураційного аудиту	Системний адміністратор	Несанкціоновані зміни	Відкат до резервної копії, розслідування
Кількість повідомлень про фішинг	Щодня	Моніторинг соціальних мереж, веб-сайтів	Адміністратор безпеки	Збільшення кількості повідомлень на 20%	Інформування громадян, блокування фішингових сайтів
Кількість інцидентів, пов'язаних з втратою даних	Що-місяця	Аналіз логів, звіти про інциденти	Адміністратор безпеки	Кожен випадок втрати персональних даних	Розслідування, інформування регулятора, відновлення даних
Час відгуку на інциденти	Що-місяця	Аналіз логів інцидентів	Керівник служби безпеки	Перевищення нормативного часу відгуку	Аналіз причин, коригування процедур реагування
Ефективність резервного копіювання	Що-місяця	Перевірка резервних копій	Системний адміністратор	Неможливість відновлення даних	Оптимізація процедури резервного копіювання
Задоволеність користувачів електронними послугами	Щоквартально	Опитування користувачів	Відділ взаємодії з громадськістю	Зниження рівня задоволеності на 10%	Аналіз причин, вдосконалення сервісів

Джерело: авторська розробка

Для ефективної роботи системи відстеження кіберзагроз необхідно враховувати низку важливих аспектів, які забезпечують всебічний захист та адаптацію до швидкозмінюваних умов кіберпростору. Першочерговим є постійний моніторинг глобальних тенденцій в області кіберзагроз. Це включає відстеження еволюції методів атак, актуальних загроз для державних інформаційних систем. Також необхідно враховувати геополітичний контекст, оскільки міжнародні конфлікти, політичні події та економічні інтереси можуть

стати катализаторами кібератак.

Комплексний підхід до безпеки вимагає об'єднання різних систем безпеки, таких як SIEM (Security Information and Event Management – управління інформацією та подіями безпеки), IDS/IPS (Intrusion Detection System / Intrusion Prevention System - система виявлення вторгнень / система запобігання вторгненням), WAF (Web Application Firewall – міжмережевий екран веб-додатків), EDR (Endpoint Detection and Response – система виявлення та реагування на загрози на кінцевих точках), для створення єдиної картини кібербезпеки органу публічної влади.

Для ефективного відстеження кіберзагроз можна використовувати різноманітні інструменти, зокрема: системи виявлення вторгнень (IDS, Intrusion Detection System) - аналізують мережевий трафік на наявність ознак атак; системи запобігання вторгненням (IPS, Intrusion Prevention System) – активно блокують атаки на мережу; захисні стіни (firewalls) – контролюють вхідний і вихідний мережевий трафік; системи управління подіями інформаційної безпеки (SIEM, Security Information and Event Management) – збирають і аналізують дані з різних джерел для виявлення загроз; програмне забезпечення для виявлення шкідливого коду (antivirus / anti-malware software) – сканує системи на наявність вірусів та іншого шкідливого програмного забезпечення; система захисту веб-додатків (WAF, Web Application Firewall) – відстежує, фільтрує та блокує http-трафік між веб-додатком та Інтернетом; система виявлення та реагування на загрози на кінцевих точках (EDR, Endpoint Detection and Response) – відстежує роботу комп'ютерів, серверів та інших пристроїв, забезпечуючи їхній захист від атак.

Інтеграція цих систем дозволяє більш ефективно виявляти та реагувати на загрози. Використання інструментів автоматизації для збору, аналізу та кореляції даних з різних джерел є критично важливим для своєчасного реагування на інциденти.

Важливим аспектом є активний обмін інформацією про загрози з іншими органами влади, правоохоронними органами та приватними компаніями. Участь

у спільних проектах з підвищення кібербезпеки дозволяє використовувати колективний досвід та ресурси для захисту від кібератак. Проведення регулярних тренінгів для персоналу з питань кібербезпеки підвищує їх обізнаність про потенційні загрози та правила безпечної роботи, що зменшує ризик успішних атак, пов'язаних з людським фактором всередині органу влади.

Сучасні технології штучного інтелекту можуть значно посилити систему моніторингу, наприклад здійснювати:

- аналіз великих обсягів даних для виявлення аномалій, які важко помітити людині;
- автоматизацію рутинних завдань, таких як аналіз логів (послідовний запис подій, що відбуваються в системі; дії користувачів, системні повідомлення, помилки, спроби доступу; логи зберігаються на серверах, мережевому обладнанні, системах безпеки та інших компонентах інформаційної системи), та класифікацію інцидентів (будь-яка подія, яка порушує або може порушити конфіденційність, цілісність або доступність інформації - несанкціонований доступ, зміна даних, випадкова або навмисна втрата даних, дії співробітників, які можуть завдати шкоди тощо);
- прогнозування потенційних загроз на основі історичних даних [142].

Отже, запропонована індикативна панель є базовою моделлю, яку можна адаптувати до конкретних потреб кожного органу публічної влади та інтегрувати у єдину національну систему координації кібербезпеки. Систематичний моніторинг, аналіз та своєчасне реагування на загрози є ключовими факторами для забезпечення безпеки цифрової взаємодії органів публічної влади та інтероперабельності інформаційних систем, як є основою для надання державних електронних послуг.

Однак, проблема координації є лише одним з викликів, що стосується більш широкого питання – *обмеженого фінансування та ресурсів*. Недостатнє фінансування та обмежені технічні ресурси державних органів, відповідальних за кібербезпеку, істотно знижують їхню здатність ефективно протидіяти кіберзагрозам. Без належного фінансового забезпечення важко впроваджувати

сучасні технології, розробляти ефективні стратегії захисту та підтримувати високий рівень готовності до нових викликів. Складність завдань у сфері кібербезпеки зростає разом із розвитком технологій, що використовуються кіберзлочинцями. Для ефективного протистояння необхідні сучасні інструменти та програмне забезпечення. Швидкість реагування на кіберінциденти є критичною, і без достатнього фінансування впровадження сучасних систем моніторингу, аналізу та попередження загроз унеможливило своєчасне виявлення та нейтралізацію атак [143].

Використання штучного інтелекту (AI) та машинного навчання (ML) в кібербезпеці становить значний прогрес у захисті інформаційних систем. Ці технології здатні обробляти великі обсяги даних з високою швидкістю, що робить їх надзвичайно ефективними для виявлення та протидії кіберзагрозам. Однією з ключових переваг AI та ML є здатність до навчання та адаптації: алгоритми постійно вдосконалюються у відповідь на розвиток нових типів загроз. Ще одним важливим аспектом є автоматизація рутинних операцій, що дозволяє фахівцям з кібербезпеки зосереджуватися на стратегічних рішеннях та плануванні реагування на інциденти. Технології AI та ML можуть автоматично виявляти аномалії та потенційні загрози, підвищуючи оперативність і точність реагування. У міру подальшого розвитку цих технологій вони дедалі більше ставатимуть критичною складовою захисту цифрових активів та інформаційних систем органів публічної влади, що потребує належного фінансового та ресурсного забезпечення.

Згідно зі звітом Cybersecurity Ventures, глобальні економічні збитки від кібератак досягнуть 10,5 трильйонів доларів США до 2025 року [144]. Крім того, для ефективного протистояння транснаціональним кіберзагрозам необхідна тісна співпраця з міжнародними організаціями та іншими країнами, що також потребує фінансових витрат.

Останні роки показали зростання кібератак на енергетичні компанії, що свідчить про високий рівень вразливості цієї сфери. Регулярно повідомляється про випадки витоку персональних даних громадян України з баз даних

державних органів. Кібератаки призводять до тимчасової недоступності державних електронних послуг, що створює незручності для громадян.

Для вирішення цієї проблеми необхідно значно збільшити бюджетні видатки на кібербезпеку, залучати приватний сектор до фінансування та реалізації проектів у цій сфері, проводити аудит витрат на кібербезпеку та оптимізувати бюджети. Розширення міжнародного співробітництва у сфері кібербезпеки дозволить отримати доступ до новітніх технологій кібернетичного захисту.

Недостатнє фінансування та технічне забезпечення органів публічної влади, відповідальних за кібербезпеку, створює не лише обмеження у протидії кіберзагрозам, а й серйозні кадрові проблеми. Це дозволяє виділити ще один важливий безпековий виклик – *нестачу кваліфікованих фахівців у сфері кібербезпеки* та обмежені можливості підвищення компетенцій тих, хто здобув освіту кілька років тому. Брак фахівців значно ускладнює ефективну боротьбу з кіберзагрозами, а ця проблема тісно пов'язана з обмеженим фінансуванням: недостатні інвестиції у розвиток людського капіталу стримують розвиток галузі та впровадження сучасних технологій.

Обмежені ресурси призводять до серйозних кадрових проблем, включаючи нестачу кваліфікованих фахівців у сфері кібербезпеки та обмежені можливості для їх підготовки. Відсутність достатньої кількості спеціалістів значно ускладнює боротьбу з кіберзагрозами, а брак спеціалізованих освітніх програм та тренінгів для підвищення кваліфікації ще більше поглиблює проблему.

Сучасні кібератаки стають все більш складними та витонченими, що вимагає від фахівців високого рівня кваліфікації та постійного оновлення знань. Технології в сфері кібербезпеки розвиваються швидкими темпами, і фахівці повинні постійно навчатися новому. Крім того, висококваліфіковані фахівці користуються великим попитом на міжнародному ринку праці, що ускладнює їхнє залучення та утримання в Україні.

Наслідки дефіциту кадрів проявляються у затримках виявлення та усунення вразливостей, неефективному реагуванні на кіберінциденти та

зростанні кількості кібератак. Недостатня кількість кваліфікованих фахівців ускладнює оперативне реагування на інциденти, створюючи сприятливі умови для діяльності кіберзлочинців. Багато випадків витоку даних пов'язані з людським фактором, коли співробітники, що не мають достатньої компетенції, допускають помилки. Відсутність фахівців з цифрової криміналістики ускладнює проведення розслідувань кіберзлочинів, а органи публічної влади відчують критичну нестачу кадрів, що негативно впливає на здатність захищати власні інформаційні системи.

Для подолання цієї проблеми необхідно впроваджувати спеціалізовані освітні програми з кібербезпеки на всіх рівнях освіти, створювати системи безперервного підвищення кваліфікації фахівців, залучати приватний сектор до підготовки кадрів та розробляти спільні навчальні програми. Заохочення молоді до обрання професії у сфері кібербезпеки, а також розвиток міжнародного співробітництва для обміну досвідом і залучення іноземних експертів, є додатковими важливими кроками для зміцнення кадрового потенціалу в галузі.

Українські університети, відомі своєю високою репутацією в галузі інформаційних технологій, пропонують підготовку фахівців з кібербезпеки. Освітні програми цих університетів включають базові дисципліни з математики, інформатики, теорії алгоритмів, операційних систем та мережевих технологій, які є фундаментом для подальшого вивчення кібербезпеки. Більшість програм пропонують можливість спеціалізації в певних напрямках кібербезпеки, таких як захист мереж, захист інформації, пентестинг, криптографія тощо. Навчальні заклади забезпечують високий рівень практичної підготовки студентів через лабораторні роботи, проекти та стажування, активно займаються науковими дослідженнями в галузі кібербезпеки, співпрацюють з іноземними партнерами, що дозволяє студентам брати участь у міжнародних програмах обміну та отримувати міжнародні сертифікати.

До прикладу, Національний технічний університет України «КПІ ім. Ігоря Сікорського» має потужну математичну та інженерну базу, що дозволяє студентам глибоко розуміти принципи роботи інформаційних систем. Київський

національний університет імені Тараса Шевченка має сильні позиції в теоретичних аспектах кібербезпеки та криптографії. Львівська політехніка відрізняється акцентом на практичній підготовці та тісними зв'язками з промисловістю. Одеський національний університет імені І. І. Мечникова має розвинені програми з захисту інформації в банківській сфері. Харківський національний університет радіоелектроніки спеціалізується на підготовці фахівців з радіоелектроніки та має відповідні лабораторії для вивчення кібербезпеки.

Система підвищення кваліфікації фахівців з кібербезпеки в Україні активно розвивається, але зіштовхується з низкою викликів. Державні університети, військові академії та приватні компанії пропонують різноманітні програми, спрямовані на підвищення рівня знань та навичок у цій галузі. Національний університет цивільного захисту України фокусується на підготовці наукових та педагогічних кадрів, надаючи їм знання з кібербезпеки для подальшого навчання студентів [145].

Також варто відзначити роль державних установ, таких як Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ), Національне агентство України з державної служби проводить навчання та тренінги для державних службовців, акцентуючи увагу на кібергігієні та реагуванні на кіберінциденти [146].

Проте, ефективність цих програм обмежена через бюрократичні перепони та недостатню фінансову підтримку.

Військові академії та інститути підвищують кваліфікацію військових фахівців, надаючи їм знання з кібербезпеки, необхідні для захисту державних інтересів. Технічні університети (КПІ, Львівська політехніка, Харківський національний університет радіоелектроніки та ін.) організують навчальні курси для ІТ-спеціалістів та науковців, надаючи їм практичні навички в галузі кібербезпеки. Національний технічний університет України «КПІ ім. Ігоря Сікорського» та Київський національний університет імені Тараса Шевченка, мають програми магістратури та аспірантури, що спеціалізуються на

кібербезпеці. Однак, програми цих закладів вищої освіти часто відстають від сучасних вимог через обмежене фінансування та недостатнє оновлення навчальних матеріалів.

Крім університетів, в Україні існують також спеціалізовані навчальні центри та курси, які пропонують програми підвищення кваліфікації для фахівців з кібербезпеки. Наприклад, компанії, що спеціалізуються на інформаційній безпеці, такі як SoftServe, Eleks та інші, проводять тренінги та сертифікаційні курси. Ці курси часто орієнтовані на практичні аспекти кібербезпеки та відповідають міжнародним стандартам, таким як сертифікації CompTIA Security+, CISSP, CEN тощо [147].

Важливою складовою системи підвищення кваліфікації є міжнародна співпраця. Українські фахівці беруть участь у міжнародних програмах обміну, конференціях та семінарах, що дозволяє їм отримувати сучасні знання та навички. Наприклад, Україна співпрацює з НАТО у рамках програми «NATO Cyber Defence Pledge», що включає навчання та обмін досвідом у сфері кібербезпеки [148].

Однак, реалізація програм підвищення кваліфікації зіштовхується з проблемою недостатнього фінансування, що обмежує їх масштаби та якість. Окрім того, відсутність єдиної державної стратегії в галузі кібербезпеки призводить до розрізненості підходів різних навчальних закладів до підвищення кваліфікації.

Отже, ефективне забезпечення кібербезпеки в Україні потребує комплексного державного підходу, що охоплює кілька ключових напрямів. По-перше, необхідно розробити єдину державну стратегію кібербезпеки, яка визначатиме пріоритети, цілі та заходи для захисту національних інформаційних систем. Така стратегія забезпечить узгодженість дій різних органів публічної влади та інших суб'єктів у сфері кібербезпеки. По-друге, важливим є вдосконалення законодавчої бази шляхом деталізації норм у сфері кібербезпеки, встановлення чітких вимог до захисту інформації та визначення відповідальності за її порушення. Це створить правові основи для ефективного реагування на

кіберзагрози та підвищить рівень відповідальності за недотримання стандартів безпеки. По-третє, критично необхідним є значне збільшення фінансування кібербезпеки для забезпечення ресурсів на придбання сучасного обладнання та програмного забезпечення, а також на підтримку наукових досліджень і розробок у цій сфері. По-четверте, розвиток кадрового потенціалу є головним чинником. Це передбачає створення спеціалізованих освітніх програм, системи постійного підвищення кваліфікації фахівців та активне залучення приватного сектору до підготовки кадрів, що дозволить формувати високопрофесійний персонал для реагування на сучасні кіберзагрози. По-п'яте, активізація міжнародного співробітництва забезпечить обмін досвідом, доступ до передових технологій та методик, а також допоможе впроваджувати кращі світові практики у сфері кібербезпеки. Крім того, посилення ролі громадянського суспільства та підвищення рівня кібергігієни серед населення сприятиме більшій обізнаності та відповідальності громадян, що підвищить стійкість та захищеність національної інформаційної інфраструктури на всіх рівнях. Комплексна реалізація цих заходів дозволить створити ефективну, стійку та надійну систему кібербезпеки, здатну протидіяти сучасним і майбутнім загрозам.

У другому розділі дослідження проаналізовано нормативно-правові та організаційні механізми цифрової взаємодії органів публічної влади України в умовах розвитку електронного урядування; охарактеризовано механізми цифрової взаємодії та інтеперабельності інформаційних систем органів публічної влади у провідних країнах світу; досліджено безпекові аспекти цифрової взаємодії у системі органів публічної влади в Україні.

Обґрунтовано, що цифрова взаємодія органів публічної влади з населенням є критично важливою для підвищення прозорості, доступності та ефективності адміністративних послуг, що сприяє інноваційному розвитку публічного управління. Глобальні тенденції та досвід розвинених країн підтверджують, що цифровізація не лише покращує ефективність публічного управління, але й забезпечує більшу відкритість уряду перед громадянами, що обумовлює

необхідність глибокого інтегрування сучасних технологій у всі аспекти публічного управління.

Доведено, що успішна цифрова трансформація потребує розвинутої законодавчої бази. В Україні ухвалено нормативно-правові акти, такі як Закон України «Про інформацію» та «Про електронні документи та електронний документообіг», які створюють правову основу для ефективного впровадження цифрових технологій у державному управлінні. Ці документи сприяють формуванню правових і організаційних умов для інтеграції новітніх технологій, що є критично важливим для успіху цифровізації. Проте, відсутність інтеграції між різними законами, що регулюють цифрову взаємодію, призводить до правової плутанини. Це підтверджується аналізом статей законів, які не завжди узгоджені між собою, що ускладнює реалізацію цифрових ініціатив.

З'ясовано, що міжнародні стандарти, такі як ISO 15489:2001 і MEK 82045-1:2001, встановлюють високі вимоги до управління документами та процесами, проте їх впровадження в Україні стикається з проблемами термінологічних і концептуальних суперечностей (ISO, 2001). Закцентовано на необхідності адаптації цих стандартів до місцевих умов, що дозволить підвищити їх ефективність і забезпечити відповідність міжнародним вимогам (ISO, 2020).

Для подолання зазначених проблем важливо реалізувати низку заходів, що підвищать роль стандартів у різних сферах, забезпечивши активізацію інформаційно-просвітницької діяльності щодо їх значення та застосування; оптимізувати процес розробки і затвердження національних стандартів, залучати зацікавлені сторони до цього процесу та використовувати ІТ-технології для підвищення ефективності; забезпечити належну оплату праці та розробити програми підвищення кваліфікації для фахівців у сфері стандартизації; залучити додаткові фінансові ресурси для розвитку системи стандартизації, що дозволить забезпечити її ефективну функціональність та адаптацію до сучасних вимог.

Показано, що цифровізація є не лише інструментом підвищення ефективності та конкурентоспроможності органів публічної влади, але й важливим засобом переформатування взаємовідносин між державою і

громадянином. Електронне урядування, будучи складовою процесу цифровізації, сприяє спрощенню доступу громадян до державних послуг, забезпечуючи взаємодію з органами влади в режимі реального часу. При цьому частка громадян, які користуються послугами електронного уряду, значно відрізняється в різних країнах, що пояснюється рівнем розвитку інфраструктури, пропозицією електронних послуг та структурними проблемами.

Доведено, що цифрова взаємодія органів публічної влади в Україні є незворотним процесом, який створює нові можливості для підвищення ефективності та прозорості державних послуг. Водночас вона супроводжується низкою безпекових викликів, серед яких виокремлено: відсутність чітких норм та стандартів кібербезпеки, що ускладнює впровадження заходів захисту; відсутність єдиної стратегії кібербезпеки та роздробленість відповідальності між органами публічної влади, що знижує ефективність координації та реагування на кіберзагрози; обмежене фінансування та недостатнє технічне оснащення, що обмежує застосування сучасних технологій і розвиток людського капіталу; дефіцит кваліфікованих фахівців, що зменшує рівень захисту інформаційних систем.

Основні результати дослідження, що викладені у другому розділі, висвітлено у таких публікаціях автора: [106; 108; 130; 142].

## **РОЗДІЛ 3. ШЛЯХИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ЦИФРОВОЇ ВЗАЄМОДІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ**

### **3.1 Запровадження інтегрованості інформаційних систем органів публічної влади як чинник удосконалення механізмів цифрової взаємодії**

Удосконалення механізмів цифрової взаємодії органів публічної влади є важливою складовою процесу формування ефективного електронного урядування. У сучасних умовах стрімкої цифровізації потреба в цілісному інформаційному просторі, у межах якого органи влади можуть здійснювати узгоджений обмін даними, набуває стратегічного значення. На нашу думку, саме інтегрованість інформаційних систем виступає головним чинником, що забезпечує системну, безперервну та безпечну взаємодію між суб'єктами публічного управління.

Інтегрованість розглядається не лише як технічна сумісність систем, а як багатовимірне явище, що охоплює технічну, семантичну, організаційну, юридичну та політичну інтегрованість. Такий підхід закріплено у Європейській рамці інтегрованості (European Interoperability Framework, EIF), яка є стратегічним документом для країн ЄС та партнерів у сфері побудови цифрових держав [149].

Водночас сучасне розуміння інтегрованості неможливе без урахування ціннісних засад цифрової трансформації. У цьому контексті важливим орієнтиром є Європейська декларація про цифрові права та принципи (European Declaration on Digital Rights and Principles, 2022), яка підкреслює пріоритетність захисту прав людини у цифровому середовищі, прозорість, безпечність та інклюзивність цифрових рішень. Документ визначає, що цифровізація має базуватися не лише на технологічних стандартах, але й на демократичних цінностях, що гарантують довіру громадян до електронних сервісів [150].

EIF також наголошує на принципах «основне цифрове ядро» (interoperability-by-design), зосередженості на потребах користувачів (user-centricity), відкритості даних, багаторівневого врядування та повторного використання існуючих рішень, що забезпечують сталість та ефективність цифрових трансформацій.

Впровадження інтероперабельності є базовою умовою створення цілісного цифрового середовища, у якому управлінські рішення приймаються на основі актуальних і достовірних даних, що безперешкодно циркулюють між усіма рівнями публічної влади. Без такого підходу неможливо досягти високої швидкості та якості надання адміністративних послуг, підвищення прозорості урядування, а також забезпечення комплексної реалізації публічної політики в умовах динамічних цифрових змін. Саме інтероперабельність як здатність різних систем, інституцій і процесів ефективно взаємодіяти виступає базовою умовою для забезпечення безперервного, безпечного та зручного обміну даними між публічними структурами [151].

EIF виокремлює п'ять взаємопов'язаних вимірів: технічний, семантичний, організаційний, юридичний та політичний. Україна, адаптуючи ці підходи до національного контексту, здійснила низку реалізованих кроків, що відображають розвиток електронного урядування через поступовий перехід до повсюдної цифровізації. Відтак, здатність органів публічної влади ефективно функціонувати в умовах розвитку електронного урядування залежить не лише від наявності технологій, а й від інтегрованої управлінської спроможності підтримувати постійний, захищений та структурований обмін інформацією.

*Технічна інтероперабельність* передбачає сумісність ІТ-систем, стандартів передачі даних, протоколів і архітектур цифрового обміну. У цьому напрямі ключовим досягненням України стало впровадження державної системи електронної взаємодії «Трембіта», яка запрацювала у 2020 році. Ця платформа функціонує як захищена шина обміну даними між державними реєстрами й інформаційними системами на основі технології X-Road. Система «Трембіта» за перші три місяці 2025 року обробила понад 2,57 млрд транзакцій, що є

рекордним показником кварталним показником [152]. З моменту запуску, станом на кінець березня 2025 року система показує понад 12,3 млрд транзакцій, з активним розширенням мережі учасників та сервісів. Впроваджені цифрові сервіси охоплюють понад 385 000 реєстрацій новонароджених (послуга «eМалятко») та понад 250 000 операцій в рамках ID-проєкту «ID-14» (отримання ID-картки та РНОКПП) [153]. Окрім того, технічна інтеграція з мобільним застосунком «Дія» дозволила об'єднати понад 130 послуг у зручному цифровому форматі.

*Семантична інтероперабельність* передбачає уніфікацію форматів, термінів і структур даних для забезпечення їхньої коректної інтерпретації та обробки в різних ІТ-системах. У цьому контексті Україна здійснює перехід до стандартизованих форматів обміну: JSON, XML для реалізації ключових державних сервісів. Важливою складовою є національний портал відкритих даних data.gov.ua який містить понад 50 тис. наборів структурованої інформації, супроводжених каталогом метаданих. Цей портал не лише підтримує принцип відкритості, але й сприяє семантичній сумісності через систематизацію ідентифікаторів, форматів і полів баз даних [154].

*Організаційна інтероперабельність* акцентує на узгодженості процедур, управлінських моделей і бізнес-процесів між органами влади. Одним із реалізованих напрямів є модернізація системи надання адміністративних послуг через розвиток ЦНАП 2.0. Ці центри працюють за принципом «єдиного вікна», а їхня інтеграція із платформою «Трембіта» забезпечує цифрову взаємодію з базами даних та реєстрами. Водночас, впроваджується підсистема «Вулик», що функціонує як внутрішня ІТ-платформа для управління процесами надання послуг у ЦНАП, зокрема за рахунок інтеграції з основними державними реєстрами [153].

*Юридична інтероперабельність* стосується гармонізації законодавчих та нормативних актів, які забезпечують законність і легітимність обміну даними між суб'єктами владних повноважень. Україна здійснила важливий крок у цьому напрямі, ухваливши Закон України «Про особливості надання публічних

(електронних) публічних послуг» № 1689-IX 2021 року, який створює правові умови для цифровізації процедур взаємодії держави з громадянами та бізнесом, зокрема щодо цифрової ідентифікації, віддаленої автентифікації та електронного документообігу [155].

Крім того, державна система електронної взаємодії «Трембіта» сертифікована відповідно до міжнародного стандарту ISO/IEC 27001, що підтверджує високий рівень інформаційної безпеки системи.

*Політична інтероперабельність* передбачає наявність стратегії, політичної волі, інституційної підтримки та довгострокової координації цифрової трансформації. У 2024 році Кабінет Міністрів України затвердив Стратегію цифрового розвитку інноваційної діяльності на період до 2030 року та операційний план її реалізації на 2025-2027 роки (розпорядження КМУ № 1351-р від 31.12.2024) [156]

Документ визначає цифрову інтероперабельність як пріоритет і містить цілі щодо розвитку інституційної та технологічної спроможності. У межах імплементації створено Координаційну раду з розвитку цифрової економіки при Міністерстві економіки України [157].

Важливу роль у досягненні результатів відіграють міжнародні ініціативи – EGOV4Ukraine, EU4DigitalUA, DT4UA, які надають технічну, аналітичну та інфраструктурну підтримку реформам у сфері електронного врядування.

Загальна орієнтація на міжвідомчу цифрову інтеграцію в Україні закріплена в Концепції розвитку електронного урядування (розпорядження КМУ № 649-р від 20.09.2017 р.) [89].

Вказаний програмний документ визначає основні напрями формування цифрової держави та особливо підкреслює, що цифрова взаємодія між органами публічної влади є однією з головних умов підвищення прозорості, ефективності та підзвітності управлінських процесів. Важливим аспектом концепції є ідея створення єдиного інформаційного середовища, яке забезпечувало б безперебійну передачу, обробку та використання даних у режимі реального часу. Це покликане усунути дублювання функцій, оптимізувати ресурси та підвищити

якість надання публічних послуг.

Закладені в Концепції підходи отримали подальший розвиток у Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року (розпорядження КМУ № 1467-р від 17 листопада 2021 року) [158].

У цьому документі детально викладено архітектурні принципи цифрової інтеграції, включаючи міжвідомчу координацію, реєстрову сумісність, а також відкритість даних і стандарти обміну. Особливу увагу приділено питанню інтероперабельності державних інформаційних систем, що розглядається не як технічне завдання, а як основа системного реформування управлінської інфраструктури.

Узагальнення бачення цифрової інтеграції також закріплено у Рамці цифрових компетентностей, розроблених Міністерством цифрової трансформації України у 2021 році [159]. У цьому документі цифрову компетентність розглянуто не лише як навички користування технікою, а як здатність взаємодіяти з державою в цифровому середовищі, розуміти принципи роботи електронних сервісів і забезпечувати відповідальне поводження з персональними даними. Таким чином, забезпечення інтероперабельності тлумачиться і як фактор цифрової інклюзії, що забезпечує рівний доступ до адміністративних послуг усім громадянам.

Ще один важливий аспект інституціоналізації міжвідомчої цифрової взаємодії відображено в Державній стратегії регіонального розвитку на 2021-2027 роки (постанова КМУ № 695 від 5 серпня 2020 року) [160]. У ній цифровізація визначається як інструмент територіального управління, що має забезпечити інтеграцію інформаційних потоків між центральним, регіональним та місцевим рівнями влади. Така інтеграція має створити умови для децентралізованої, але скоординованої політики, де цифрова інфраструктура підтримує прозорість регіональних бюджетів, ефективність сервісів та підзвітність органів місцевого самоврядування.

Отже, поступове нарощування правового, інституційного та

технологічного потенціалу цифрової взаємодії в Україні базується на системних документах, які послідовно відображають перехід до інтероперабельного, відкритого та клієнтоцентричного електронного урядування [161].

Таким чином, аналіз реалізованих кроків свідчить, що Україна поступово впроваджує підходи, закладені в EIF, трансформуючи міжнародні стандарти в конкретні механізми цифрової взаємодії. Це дозволяє не лише покращити координацію між органами влади, але й закласти основу для подальшого розвитку електронного урядування, відкритого до громадян, безпечного, доступного та ефективного [162]. У нижченаведеній табл. 3.1 систематизовано, як міжнародні підходи інтероперабельності (зокрема, EIF) трансформуються у практику національного електронного урядування через конкретні реалізовані ініціативи, нормативні документи та інфраструктурні рішення.

*Таблиця 3.1*

Міжнародні підходи до інтероперабельності та їх реалізація в Україні

<b>Тип інтер-операбельності</b>	<b>Підхід у міжнародній практиці (згідно з EIF)</b>	<b>Впровадження в Україні</b>
<b>Технічна інтер-операбельність</b>	Сумісність ІТ-систем, протоколів і обміну даними через технічні шини	Платформа «Трембіта» – державна шина обміну даними, запущена 2020 року, сервіс обслуговує понад 200 органів, понад 3 млрд транзакцій Інтеграція з додатком «Дія» – понад 130 державних послуг, онлайн-паспорти з 2020р.
<b>Семантична інтер-операбельність</b>	Узгодженість форматів і термінів для коректної інтерпретації даних	Перехід до структурованих форматів (JSON, XML) для ключових сервісів Каталог метаданих та відкриті набори даних на <a href="http://data.gov.ua">data.gov.ua</a>
<b>Організаційна інтер-операбельність</b>	Скоординовані бізнес-процеси та процедурні моделі між держорганами	Центри ЦНАП 2.0, де діють принципи «єдиного вікна» з підтримкою цифрової інтеграції; Підключення адміністративних центрів до «Вулика», асоційованого з «Трембіта»

## Продовження таблиці 3.1

<b>Юридична інтер-операбельність</b>	Гармонізація правових норм для легального обміну інформацією	Закон України «Про особливості надання публічних (електронних публічних) послуг» Відповідність систем категорії ISO/IEC 27001 – підтверджено у «Трембіта»
<b>Політична інтер-операбельність</b>	Забезпечення політичної підтримки, координації та довгострокового бачення	Розпорядження КМУ від 31 грудня 2024 р. № 1351-р «Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках»; Створення координаційної Ради з розвитку цифрової економіки; Партнерства: EGOV4Ukraine, EU4DigitalUA, DT4UA за підтримки ЄС і eGA

Джерело: складено автором

Очевидно, що усі компоненти інтероперабельності певною мірою інтегровані в систему електронного урядування України, що свідчить про стратегічну орієнтацію держави на відповідність європейським стандартам, зокрема EIF. Ключові досягнення, як-от функціонування платформи «Трембіта», запуск і розвиток мобільного застосунку «Дія», гармонізація законодавства у сфері електронних публічних послуг, а також схвалення Стратегії цифрового розвитку до 2030 року демонструють політичну волю та системний підхід до цифрової трансформації.

Проте, попри загальний поступ, впровадження інтероперабельності в Україні залишається нерівномірним і потребує додаткового інституційного, технічного та нормативного доопрацювання.

Семантична інтероперабельність ще не досягла належного рівня стандартизації. Уніфікація термінології, форматів метаданих, а також інтеграція

реєстрів через узгоджені словники та онтології реалізується фрагментарно. Портал відкритих даних data.gov.ua містить значну частину інформації у неформалізованому або застарілому вигляді. Організаційна інтероперабельність стримується відсутністю єдиних регламентів управлінських процесів між органами влади. У багатьох ЦОВВ немає чітко визначених процедур цифрової взаємодії, а моделі інтеграції не завжди масштабовані. Юридична інтероперабельність, хоча й має базове законодавче підґрунтя, стикається з проблемами гармонізації відомчих нормативно-правових актів, а також недостатньою швидкістю адаптації правової бази до нових цифрових рішень (наприклад, регулювання штучного інтелекту, хмарних сервісів, big data). Політична інтероперабельність, хоча формально підтримується на високому рівні, залежить від стабільності політичної ситуації, пріоритетності цифрової трансформації в урядовому порядку денному та послідовності фінансування проєктів. Моніторинг і зворотний зв'язок щодо ефективності реалізованих рішень наразі недостатньо інституціоналізовані. Індикатори інтероперабельності, хоча і декларуються в окремих звітах (наприклад, у межах міжнародної технічної допомоги), не охоплюють усі виміри і не публікуються регулярно.

Однак, незважаючи на недоліки, Україна перебуває на стадії переходу від фрагментарних рішень до комплексної моделі інтероперабельності. Для досягнення повної відповідності європейським стандартам важливо посилити інституційну спроможність органів публічної влади, забезпечити єдині технічні та семантичні стандарти, а також вивести моніторинг цифрової взаємодії на рівень постійно діючого механізму управлінського аналізу [163].

Як зазначалось у попередніх розділах роботи, реалізація ефективної цифрової взаємодії в системі публічного управління передбачає не лише технічну сумісність інформаційних систем, а й чітке розуміння характеру, напрямів і функціонального навантаження інформаційних потоків між суб'єктами владних повноважень. Структурований аналіз таких потоків дозволяє виявити вузькі місця в обміні даними, визначити критичні точки інтеграції, а

також забезпечити оптимальне удосконалення цифрових механізмів управління.

У публічному управлінні інформаційні потоки виконують не лише сервісну функцію, а й відіграють роль механізмів стратегічного управління, моніторингу, контролю та координації. Їх ефективність безпосередньо залежить від наявності загальних стандартів обміну, спільної термінології та узгоджених технічних протоколів, що передбачено у EIF. Для цілісного розуміння цифрової взаємодії між суб'єктами публічної влади пропонується наступна функціональна типологізація інформаційних потоків.

*Вертикальні інформаційні потоки* формуються у межах ієрархічної структури публічного управління: від центральних органів виконавчої влади (Кабінету Міністрів України, ЦОВВ) до обласних, районних державних адміністрацій, органів місцевого самоврядування та у зворотному напрямі. Їх зміст охоплює інформування щодо ухвалених документів, політичних рішень, стандартів та нормативів; отримання звітів, аналітики та даних моніторингу; а також надання рекомендацій чи приписів для виконання. До прикладу, у сфері освіти вертикальні потоки реалізуються через цифрові платформи збору, консолідації та валідації статистичних і оперативних даних щодо контингенту учнів, ресурсного забезпечення, результатів моніторингу якості освіти.

*Горизонтальні інформаційні потоки* виникають між органами, які не перебувають у безпосередній вертикальній залежності, але потребують узгоджених дій у межах реалізації міжвідомчих політик. Вони є основою для взаємного обміну службовою інформацією, спільного адміністрування процесів (зокрема, реєстрації бізнесу, обігу нерухомості), а також кризового реагування. Значна кількість таких потоків є базовою умовою надання інтегрованих адміністративних послуг, які потребують доступу до даних одразу з кількох джерел: податкових органів; державних реєстрів тощо. Проте, як засвідчив аналітичний звіт проєкту EGOV4UKRAINE (2021) [164], понад 50% державних сервісів в Україні залежать від міжвідомчої взаємодії, і лише третина з них функціонує в автоматизованому режимі, що свідчить про системну нестачу інтегрованості.

*Внутрішньоорганізаційні інформаційні потоки* циркулюють усередині одного органу влади між його департаментами, підрозділами та територіальними представництвами. Вони охоплюють процеси внутрішнього документообігу, погодження управлінських рішень, обміну службовою інформацією. Їх цифровізація дозволяє суттєво скоротити час прийняття рішень, усунути дублювання функцій та забезпечити підзвітність службових дій. У Мінцифри такі потоки реалізуються через впровадження інтегрованих систем електронного документообігу, які підтримують повний життєвий цикл документів: від створення до архівації.

*Транскордонні інформаційні потоки* охоплюють взаємодію українських органів влади з міжнародними інституціями, що стає дедалі актуальнішим на тлі руху України до інтеграції з ЄС. Ці потоки передбачають доступ до європейських цифрових платформ, використання міжнародних стандартів даних, синхронізацію національних адміністративних сервісів з європейськими інтерфейсами. Зокрема, участь України у пілотних проектах EU eHealth Digital Service Infrastructure (eHDSI) [165] сприяє створенню умов для транскордонного обміну медичними даними, а інтеграція до Single Digital Gateway [166] забезпечить громадянам і бізнесу доступ до цифрових адміністративних процедур на єдиному європейському просторі.

*Зовнішні (громадські та міжсекторальні) інформаційні потоки* забезпечують взаємодію між органами публічної влади та громадянами, підприємствами, громадськими організаціями, науковими установами. Вони формуються через платформи електронної демократії, відкриті державні реєстри, кабінети платників, мобільні застосунки та цифрові сервіси типу «Дія». Такі потоки не лише обслуговують запити користувачів, а й виконують аналітичну функцію, дозволяючи органам влади реагувати на суспільні запити в реальному часі.

Таким чином, запропонована типологізація інформаційних потоків (рис. 3.2) створює аналітичне підґрунтя для розробки архітектурної моделі механізмів цифрової взаємодії на засадах інтероперабельності. Обґрунтування, який тип

потоків потребує найбільшої уваги (наприклад, горизонтальні з точки зору міжвідомчої інтеграції; або транскордонні з погляду європейського співробітництва), дозволяє більш точно визначати пріоритетні напрями реформ.



Рис. 3.2 Типологізація інформаційних потоків

Джерело: авторська розробка

Оскільки інформаційні потоки обумовлюють виконання різноманітних завдань на різних рівнях взаємодії між органами влади, виникає об'єктивна потреба в адаптації цих потоків до нових умов цифрової трансформації публічного управління. Від звичної автоматизації існуючих процедур це відрізняється кардинально: йдеться про фундаментальне реформування (*реінжиніринг*) процесів із метою досягнення нових характеристик ефективності, швидкості, прозорості та клієнтоорієнтованості.

В українській науковій літературі цей напрям розглядається як потужний інструмент трансформації. Ю.Хромова у своїй праці акцентує на необхідності комплексного підходу до реінжинірингу: він має передбачати не лише оптимізацію процесів через цифрові засоби, а й формування нових організаційних моделей, сервісної культури та інфраструктури, в тому числі на місцевому рівні [167].

У практиці реінжинірингу процесів публічного управління дедалі ширше застосовуються підходи, засновані на моделюванні поточного стану процесів, зокрема через моделювання стану «як є» (AS-IS) та проектування бажаного стану «як має бути» (TO-BE). Такий підхід дозволяє не лише виявити слабкі місця в існуючих структурах, а й обґрунтовано прогнозувати ефекти від цифрових трансформацій.

У дослідженні італійських вчених Ф.Сімпі, М.Фараоні та ін. (Francesco Ciampi, Monica Faraoni) акцент зроблено на коеволюції цифровізації та організаційної гнучкості в публічному секторі. Автори показують, що цифрові зміни впливають не лише на технічну інфраструктуру, але й глибоко трансформують управлінські моделі, стилі прийняття рішень і міжструктурну взаємодію. Одним із основних інструментів у цьому контексті стало використання симуляційних моделей, зокрема в Італії, де до впровадження нових цифрових рішень в органах влади було проведено моделювання управлінських процесів, що дало змогу заздалегідь оцінити наслідки змін, оптимізувати ресурсне забезпечення та зберегти якість надання публічних послуг [168]. Результати цієї практики підтвердили високу ефективність моделювання як превентивного аналітичного інструменту. Зокрема, це дозволило уникнути організаційних ризиків, покращити управлінську координацію та підвищити результативність процесів без втрати функціональної цілісності.

Для України цей підхід має стратегічну цінність. Його застосування може суттєво підвищити якість цифрової трансформації, зокрема:

- у процесі проектування інтероперабельних механізмів цифрової взаємодії між органами публічної влади;

- під час розроблення та тестування оціночних моделей ефективності функціонування оновлених процесів;
- у впровадженні пілотних цифрових ініціатив з подальшим масштабуванням на всю систему публічного управління.

Важливо зазначити, що сучасні тренди об'єднують реінжиніринг із цифровими технологіями наступного покоління. Зокрема, застосування SMART-систем та штучного інтелекту (ШІ) створює передумови для автоматизації рутинних операцій, обробки великих масивів даних та прийняття проактивних рішень, автоматизує рутинні операції, а й підвищує прозорість, підзвітність і якість надання адміністративних послуг. Ці технології забезпечують проактивність, швидкість і прозорість взаємодії між владою та громадянами, що стає основою нової моделі публічного сервісу.

Згідно з аналітичним звітом Світового банку GovTech Maturity Index 2022, впровадження SMART-інструментів (електронні черги, автоматизовані реєстри, онлайн-запити) в органах публічної влади дозволяє скоротити час реагування на звернення громадян на 30-50%, а також значно зменшує навантаження на держслужбовців. У звіті акцентується, що ці зміни не лише підвищують ефективність, а й знижують ризики корупції завдяки мінімізації ручного втручання в обробку запитів. Цей підхід набуває системного характеру в країнах із високим рівнем цифрової зрілості, і його доцільно адаптувати для України [169].

У доповіді ОЕСР Governing with Artificial Intelligence (2024) висвітлено потенціал ШІ як інструменту підтримки державного управління. Зокрема, системи штучного інтелекту використовуються для прогнозування транспортних навантажень, виявлення зловживань у соціальних програмах, аналітики поведінкових даних громадян та оптимізації бюджетного планування. Так, у Сінгапурі система ШІ в реальному часі прогнозує дорожні затори та змінює режими роботи транспорту, що зменшує соціальні витрати та підвищує мобільність [170].

Європейські ініціативи також демонструють, що використання цифрових

технологій обумовлюють не лише ефективність, але й демократичну підзвітність. За даними Digital Public Administration Factsheets – 2023, відкриті дані, інтерактивні дашборди, автоматизовані аналітичні звіти та онлайн-платформи для зворотного зв'язку із громадянами сприяють зміцненню довіри до влади та зменшують інформаційний розрив між державою та суспільством. Це відповідає концепції «відкритого уряду», яку підтримують більшість країн ЄС [171].

UN E-Government Survey 2024 є 13-м щорічним глобальним звітом Організації Об'єднаних Націй, підготовленим Департаментом економічних і соціальних питань (UN DESA) [172]. У документі проводиться всебічний аналіз стану і динаміки розвитку цифрового урядування в 193 країнах-членах ООН, оцінюючи їх за допомогою комплексного індексу EGDI (E-Government Development Index). Цей індекс включає три основні компоненти: Online Service Index (OSI), що відображає якість державних електронних сервісів; Telecommunication Infrastructure Index (TII), який оцінює доступність та сталість телекомунікативної інфраструктури; а також Human Capital Index (HCI), що вимірює рівень освіти та цифрової грамотності населення.

У 2024 році індекс EGDI було доповнено новими показниками – Local Online Service Index (LOSI), який оцінює якість і доступність електронних сервісів на місцевому рівні, та компонентом e-government literacy, що фокусується на здатності громадян користуватися цифровими послугами. Це нововведення підкреслює важливість не лише загальнодержавних ініціатив, а й розвитку цифрового урядування на рівні органів місцевого самоврядування, що особливо актуально в контексті процесів децентралізації.

Основні висновки Survey 2024 демонструють стабільний глобальний прогрес у сфері цифрового уряду: частка населення, яке не користується цифровими державними послугами, скоротилася з 45% у 2022 році до 22,4% у 2024 році. Лідерами цифрового урядування традиційно залишаються країни, такі як Данія, Естонія, Сінгапур, Республіка Корея та Ісландія. Проте, хоча Європа зберігає статус найбільш розвиненого регіону, найбільш швидке зростання EGDI

відзначається в Азії. Водночас світова статистика звертає увагу на існування значного цифрового розриву – близько 1,7 мільярда людей досі залишаються поза межами якісного доступу до цифрових послуг [172].

Важливою інновацією звіту є представлення Digital Government Model Framework – екосистемного підходу до планування, впровадження і оцінки цифрових ініціатив у сфері публічного управління. Ця модель акцентує увагу на принципах прозорості, інклюзивності та кібербезпеки, підкреслюючи необхідність інтеграції технологічних, організаційних та людських ресурсів у рамках комплексної системи цифрового уряду.

З огляду на наведені дані, UN E-Government Survey 2024 має важливе значення для України. По-перше, індекси EGDI та LOSI можуть служити національними бенчмарками для оцінки та порівняння рівня розвитку електронного урядування в країні з міжнародними стандартами і практиками. По-друге, увага до локального рівня через LOSI відображає стратегічну необхідність розвитку цифрових сервісів у межах децентралізованих органів влади, що співпадає із завданнями адміністративно-територіальної реформи. По-третє, додатковий показник e-government literacy вказує на критичну важливість підвищення цифрової грамотності серед населення як умови ефективного використання електронних сервісів.

З іншого боку, звіт акцентує увагу на потенційних ризиках та викликах, які супроводжують цифрову трансформацію. Серед них – питання кібербезпеки, захисту персональних даних, забезпечення рівного доступу до цифрових технологій, а також розвиток політик, що гарантують справедливість і прозорість цифрових процесів. Саме тому екосистемний підхід Digital Government Model Framework передбачає системну інтеграцію цих аспектів у стратегії цифрового розвитку [172].

Таким чином, UN E-Government Survey 2024 є не лише статистичним звітом, а виступає потужним інструментом стратегічного планування і моніторингу цифрової зрілості держави. Для України використання його висновків і рекомендацій відкриває можливості для науково обґрунтованої

імплементації передових світових практик та формування ефективної, прозорої і інклюзивної моделі електронного урядування. Однак, для досягнення максимального ефекту необхідно системно вирішувати питання безпеки, етики та професійної готовності кадрів до роботи в умовах цифрової реальності.

Як показує світова та вітчизняна практика, реінжиніринг цифрових процесів в органах публічної влади вимагає не лише переосмислення змісту управлінських функцій, а й створення відповідного технічного та архітектурного середовища, здатного забезпечити сталу взаємодію між різнорівневими системами.

Актуальність цього підходу обумовлена тим, що сучасна цифрова взаємодія виходить далеко за межі локальних ІТ-рішень та потребує забезпечення безперервного, захищеного й стандартизованого обміну даними між різними органами публічної влади, як у вертикальному, так і горизонтальному вимірах.

З огляду на складну багаторівневу структуру цифрової взаємодії в публічному управлінні, типологічне розмаїття інформаційних потоків, а також сучасні підходи до реінжинірингу управлінських процесів із використанням SMART-систем та штучного інтелекту, постає потреба у обґрунтуванні та розробці цілісної архітектурної конструкції, яка б поєднувала організаційні, функціональні та технологічні компоненти цифрової взаємодії. У цьому контексті доцільним є розроблення архітектурної моделі механізмів цифрової взаємодії на засадах інтеперабельності інформаційних систем органів публічної влади, яка має ґрунтуватися на певних технічних та інституційних принципах, серед яких особливе значення мають:

- сервісно-орієнтована архітектура (Service-Oriented Architecture, SOA);
- використання відкритих API (Application Programming Interfaces – взаємодії, при якому органи публічної влади надають іншим організаціям (державним або приватним) стандартизовані інтерфейси доступу до своїх цифрових сервісів, даних або функціоналу);
- стандартів сумісності (*технічна* – можливість систем фізично

взаємодіяти (через мережу, формати файлів, API; *семантична* – однакове трактування даних (наприклад, що таке «особа», «адреса», «платник» у різних системах); *організаційна* – узгоджені правила взаємодії між структурами, які володіють системами; *юридична* – у європейській практиці такі стандарти кодифіковано у European Interoperability Framework (EIF), який Україна поступово адаптує через законодавчі та нормативні зміни; *політична* – довгострокової координації цифрової трансформації у сферах [173];

– впровадження міжреєстрових шлюзів (спеціальний технічний механізм, який дозволяє різним державним реєстрам (наприклад, реєстру податкових платників, земельного кадастру, реєстру юридичних осіб) обмінюватися даними в автоматизованому режимі, навіть якщо вони створені на різних платформах або розроблені різними установами.

Архітектурна модель механізмів цифрової взаємодії на засадах інтероперабельності у цьому випадку постає як концептуальна схема, що відображає взаємодію декількох основних архітектурних компонентів: цільово-функціонального (визначення завдань та повноважень органів влади), інформаційного (структура та потоки управлінських даних), сервісного (механізми надання електронних послуг, відкриті API, міжвідомчі реєстрові інтеграції) та інфраструктурного (мережева, програмна й технічна сумісність, вимоги до безпеки), кадрово-ресурсного тощо. Такий підхід є усталеним у міжнародній практиці цифрової трансформації публічного управління та дозволяє враховувати як організаційні, так і технологічні аспекти забезпечення інтероперабельності.

Як зазначалось вище, EIF містить чіткі принципи, рівні та моделі для забезпечення сумісності цифрових систем публічного сектору. Вона орієнтує держави-члени ЄС на застосування стандартизованих архітектур, відкритих інтерфейсів (open APIs), реєстрових шлюзів та сервісно-орієнтованих підходів (SOA) як ключових передумов міжвідомчої інтеграції.

Аналогічні підходи закріплені також у міжнародних методологіях цифрового архітектурного планування, таких як TOGAF (The Open Group

Architecture Framework) [174] і Government Enterprise Architecture [175], рекомендованих Світовим банком, OECD та іншими міжнародними організаціями як інструменти стратегічного управління цифровими змінами в державному секторі.

Таким чином, інтероперабельність інформаційних систем органів публічної влади виступає як методологічна рамка, що забезпечує узгоджене функціонування цифрових рішень на різних рівнях управління.

Метою механізмів цифрової взаємодії органів публічної влади на засадах інтероперабельності є створення уніфікованого, масштабованого та безпечного інформаційного середовища, яке забезпечує ефективний, прозорий та безперервний обмін управлінськими даними між усіма рівнями влади, сприяє оптимізації процесів публічного управління та підвищенню якості публічних послуг, орієнтованих на потреби громадян та суспільства. В основу їх функціонування покладено принципи: клієнтоцентричності, яка ставить в центр уваги потреби та зручність користувачів цифрових послуг; відкритості та прозорості, що гарантує доступність інформації та контролю з боку суспільства; безпеки і захисту інформації на всіх етапах її обробки та передачі; адаптивності й гнучкості, що дозволяє швидко реагувати на технологічні та організаційні зміни; системності, яка поєднує технологічні, організаційні та кадрові аспекти у цілісний комплекс.

*Цільово-функціональний механізм (організаційна архітектура)* окреслює управлінські функції органів державної влади та органів місцевого самоврядування, типові бізнес-процеси (зокрема, надання адміністративних послуг, реєстрація об'єктів, видача дозволів), а також стратегічні орієнтири цифрової трансформації, такі як прозорість, підзвітність і ефективність. В українському контексті реалізація цього рівня здійснюється на основі положень Концепції розвитку електронного урядування (2017), цифрових стратегій ЦОВВ (зокрема, Міністерства цифрової трансформації, МОН, МВС, Мінсоцполітики), а також через впровадження методологій бізнес-моделювання за стандартами BPMN (Business Process Model and Notation), які дозволяють структурно

описувати, аналізувати та оптимізувати управлінські процедури.

*Інформаційно-комунікативний механізм (інформаційна архітектура)* регламентує обіг, структуру та стандартизацію даних, що циркулюють між органами публічної влади. Цей механізм охоплює персональні, реєстрові, аналітичні дані, метадані та формати звітності. Ключовими елементами тут є стандарти сумісності (X-Road, eDelivery, UBL, RDF), які забезпечують як семантичну, так і технічну інтеграцію. В Україні цей рівень реалізується через впровадження системи «Трембіта», яка забезпечує безпечний міжвідомчий обмін даними, активний перехід до структурованих форматів (JSON, XML), а також розвиток каталогів на Єдиному порталі відкритих даних, що створює умови для прозорості та відкритості адміністративної інформації.

*Сервісно-інтеграційний механізм (прикладна архітектура)* зосереджений на інструментах реалізації управлінських функцій через цифрові сервіси та програмні інтерфейси. Цей механізм охоплює електронні сервіси для громадян і бізнесу, міжвідомчі API, реєстрові шлюзи, системи електронного документообігу (СЕД), CRM-системи. В Україні даний рівень знаходить своє втілення у таких рішеннях, як національна платформа «Дія», що забезпечує комплексний доступ до публічних сервісів, інтеграційна взаємодія реєстрів на основі API, а також розвиток сучасних фронт-офісів у межах ЦНАП 2.0, які надають послуги за принципом єдиного вікна із цифровою підтримкою всіх етапів.

*Інфраструктурно-технологічний механізм (технічна архітектура)*, який забезпечує фундаментальні технічні умови для безперебійної цифрової взаємодії. До його компонентів належать серверні платформи, хмарна інфраструктура, телекомунікативні протоколи, засоби кіберзахисту, механізми аутентифікації та авторизації (наприклад, Mobile ID, кваліфікований електронний підпис). Впровадження цих елементів в Україні здійснюється через функціонування дата-центру GOV.UA, реалізацію принципу Cloud First у публічному секторі, а також розробку стандартів інформаційної безпеки відповідно до положень Національного координаційного центру кібербезпеки

(НКЦК) та регламентів Державної служби спеціального зв'язку та захисту інформації України.

*Кадрово-ресурсний механізм (архітектура людського капіталу)* визначає людські, організаційні та управлінські ресурси, необхідні для реалізації цифрових трансформацій та підтримки інтегрованості. До цього механізму входять підготовка і підвищення кваліфікації публічних службовців у сфері цифрових компетенцій, формування міжвідомчих команд для управління цифровими проектами, а також розвиток культури цифрової трансформації. В Україні цей рівень підтримується через освітні ініціативи, зокрема курси з цифрової грамотності, розробленими Мінцифри, впровадження систем управління знаннями у ЦОВВ, а також формування спільнот практики, що сприяють обміну досвідом і найкращими практиками у сфері електронного урядування.

Архітектурна модель механізмів цифрової взаємодії на засадах інтегрованості інформаційних систем органів публічної влади (рис. 3.3) в такій конфігурації виконує низку основних функцій:

- по-перше, вона забезпечує уніфікований методологічний підхід до побудови цифрової взаємодії в публічному секторі;
- по-друге, вона формує масштабовану структуру, здатну до подальшої інтеграції з європейським цифровим простором відповідно до положень EIF;
- по-третє, вона підсилює горизонтальну та вертикальну координацію між різними рівнями органів публічної влади.

У сукупності ці компоненти утворюють основу для сталого розвитку електронного урядування, адаптованого до викликів цифрової доби та орієнтованого на потреби громадян і суспільства.

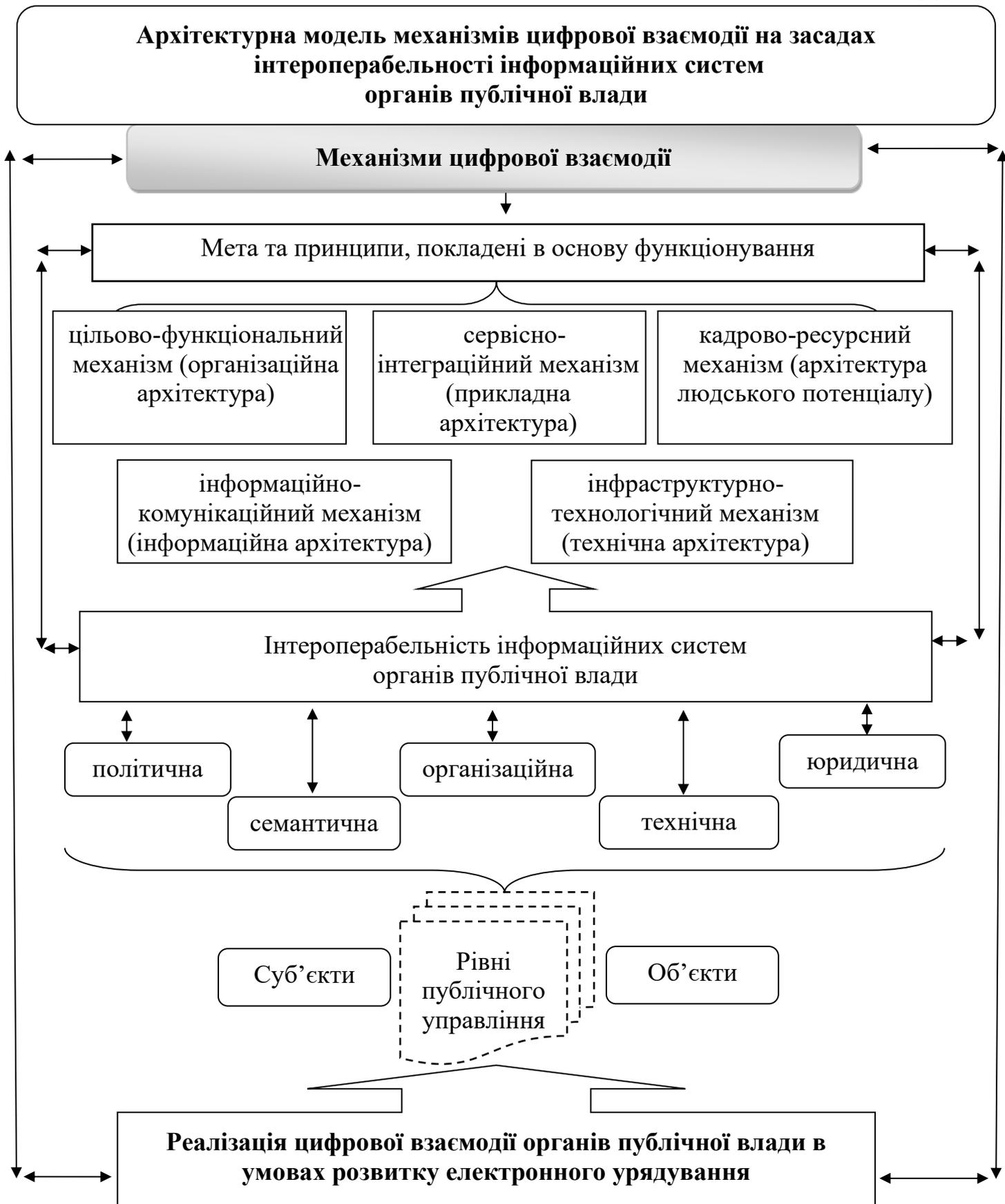


Рис.3.3. Архітектурна модель механізмів цифрової взаємодії на засадах інтероперабельності інформаційних систем органів публічної влади

Джерело: складено автором

Сучасний розвиток електронного урядування в Україні вимагає не лише технічних новацій, а й системного підходу до публічного управління, який ґрунтується на комплексній взаємодії організаційних, інформаційних, технологічних та кадрово-ресурсних складових. Вважаємо, що розвиток механізмів інтероперабельності інформаційних систем відкриває нові горизонти для підвищення ефективності публічного управління, забезпечуючи цілісний простір для обміну даними, оперативного прийняття рішень і взаємодії на всіх рівнях влади. При цьому інтерактивна міжвідомча координація та взаємодія, підтримані якісним кадровим ресурсом, виступають каталізаторами інновацій та сприяють формуванню відкритого, прозорого управління.

Таким чином, розвиток електронного урядування повинен бути зорієнтований на баланс між технологічними інноваціями і соціальними аспектами, такими як цифрова інклюзія, забезпечення кібербезпеки та захист персональних даних. Важливо, що національні ініціативи у сфері розвитку електронного урядування активно інтегруються у європейський і світовий контекст, що не лише стимулює впровадження передових практик, а й підвищує міжнародний імідж України як держави, яка прагне до високих стандартів управління.

### **3.2. Матриця моніторингу функціонування механізмів цифрової взаємодії органів публічної влади як оціночна методика у досліджуваній сфері**

Механізми цифрової взаємодії органів публічної влади, що реалізуються на засадах інтероперабельності, виступають не лише засобами технологічної трансформації, а й об'єктами постійного вдосконалення і стратегічного аналізу. В умовах швидкого розвитку цифрових технологій, зростаючих очікувань громадян та викликів кібербезпеки, особливої ваги набуває питання постійного, системного моніторингу функціонування таких механізмів. Оцінювання ефективності цифрової взаємодії не можна зводити лише до технічних

параметрів або кількісних показників використання ІКТ. Потрібен комплексний підхід, що дозволяє інтегрувати технологічні, організаційні, правові та соціальні аспекти в єдину аналітичну площину [176].

Для визначення основних чинників, які впливають на спроможність публічного сектору до впровадження та ефективного використання системи моніторингу функціонування механізмів цифрової взаємодії органів публічної влади доцільним є застосування інструментарію SWOT-аналізу (табл. 3.2), який надає змогу виявити сильні сторони, які можуть слугувати основою для подальшого масштабування цифрових ініціатив; ідентифікувати критичні слабкі сторони, що потребують першочергового усунення для забезпечення стійкості системи; визначити можливості для залучення зовнішніх ресурсів, партнерств і технологій, що сприятимуть розвитку моніторингової спроможності; проаналізувати загрози, які можуть поставити під ризик ефективність цифрової взаємодії, зокрема в умовах нестабільного середовища або обмеженого фінансування.

Таблиця 3.2

SWOT-аналіз спроможності публічного сектору до впровадження моніторингу функціонування механізмів цифрової взаємодії органів публічної влади

<p><b>Сильні сторони (Strengths)</b></p>	<ul style="list-style-type: none"> <li>– наявність досвіду реалізації цифрових платформ («Дія», «Трембіта»);</li> <li>– централізоване управління цифровими проектами (мінцифри);</li> <li>– розвинена мережа ЦНАПів;</li> <li>– дедалі більша підтримка цифровізації з боку громадськості.</li> </ul>	<p><b>Слабкі сторони (Weaknesses)</b></p>	<ul style="list-style-type: none"> <li>– фрагментарність підходів до цифровізації в окремих ОМС;</li> <li>– недостатній рівень цифрових компетентностей публічних службовців;</li> <li>– обмеженість кадрових та фінансових ресурсів на місцях;</li> <li>– інертність старих управлінських практик.</li> </ul>
--	--	---	--

## Продовження таблиці 3.2

<b>Можливості (Opportunities)</b>	<ul style="list-style-type: none"> <li>– розширення цифрових компетенцій через освітні програми;</li> <li>– впровадження «цифрової інституційної культури»;</li> <li>– використання інструментів моніторингу для управлінських рішень;</li> <li>– підтримка з боку міжнародних проєктів.</li> </ul>	<b>Загрози (Threats)</b>	<ul style="list-style-type: none"> <li>– опір змінам через страх втрати повноважень або відповідальність;</li> <li>– високий ризик «цифрової нерівності/розриву» між територіями громад;</li> <li>– обмеження бюджетів для підтримки та оновлення іт-інфраструктури;</li> <li>– залежність від сторонніх технологічних рішень.</li> </ul>
-----------------------------------	---	--------------------------	---

Джерело: авторська розробка

Таким чином, SWOT-аналіз показує, що в Україні сформовано базові передумови для впровадження національної системи моніторингу функціонування механізмів цифрової взаємодії органів публічної влади: наявні приклади успішних цифрових ініціатив, інституційна підтримка з боку центральних органів виконавчої влади, зростаючий запит суспільства на прозорі цифрові сервіси.

В сучасному публічному управлінні спостерігається тенденція до переходу від ситуативного аналізу окремих цифрових ініціатив до впровадження систем оцінювання зрілості, сталості та результативності цифрових процесів на основі визначених індикаторів. Цей підхід розглядається не лише як сукупність нових технологічних рішень, а як системна управлінська категорія, що потребує постійного вимірювання, оцінки та коригування. Як наголошують Н.Бондарчук та Н.Дуброва, цифровізація публічного управління в Україні дедалі більше сприймається як інструмент досягнення управлінської ефективності, прозорості та підзвітності, що вимагає цілеспрямованих моніторингових підходів, здатних фіксувати динаміку змін і на рівні технологій, і у кадрово-інституційній

площині [177].

При цьому особливої важливості набуває розробка національних підходів до моніторингу, які мають враховувати специфіку українського контексту, стратегічні цілі цифровізації, інституційну спроможність органів публічної влади та наявне нормативно-правове середовище. Зокрема, Закон України «Про особливості надання публічних (електронних публічних) послуг» визначає обов'язок органів публічної влади забезпечувати відкритість, зручність, безперервність і захищеність електронної взаємодії електронних ресурсів, що вимагає системної оцінки ефективності функціонування відповідних механізмів на постійній основі [155].

У цьому контексті функціонування механізмів цифрової взаємодії має спиратися на структуровану методикау, яка поєднує кількісні і якісні показники, враховує рівень відкритості органів влади, ступінь інтегрованості цифрових платформ, відповідність технічним стандартам безпеки та здатність систем реагувати на управлінські виклики. Саме тому пропонується використання матриці моніторингу як аналітичного інструменту, здатного системно відображати динаміку й ефективність функціонування цифрових механізмів на різних рівнях публічного управління. Матричний підхід, як зазначають О.Коваленко та В.Хрутьба, дозволяє розглядати процес цифрової трансформації як комплекс змін, що охоплює не лише технічну, а й організаційно-культурну, нормативну та управлінську складові, вимагаючи постійної інституціональної адаптації до нових викликів [178].

Таким чином, моніторинг функціонування механізмів цифрової взаємодії постає як центральний елемент управління цифровою трансформацією. Його результати мають безпосередній вплив на стратегічне планування, розподіл ресурсів, розвиток цифрових компетентностей, а також на формування довіри громадян до цифрових сервісів. Упровадження національно орієнтованої, емпірично обґрунтованої матриці моніторингу дозволяє перейти до якісно нового рівня управління цифровою взаємодією в публічному секторі.

Методологія побудови матриці моніторингу функціонування механізмів

цифрової взаємодії органів публічної влади спирається на поєднання трьох фундаментальних підходів: системного аналізу, емпіричної обґрунтованості та адаптивності до цифрових змін.

*Системний аналіз* передбачає, що цифрові механізми слід оцінювати як інтегровані компоненти взаємопов'язаного середовища: технічної інфраструктури, правової бази, організаційної структури та соціальних взаємовідносин. Цей підхід цілком відповідає міжнародним нормативним та методологічним орієнтирам. Зокрема, у стратегічному документі «Цифрове десятиліття Європи: Цифрові цілі на 2030 рік» (Europe's Digital Decade: Digital Targets for 2030) [179] наголошується на необхідності інтеграції цифрових технологій в усі сектори економіки та публічного управління з акцентом на інтероперабельність, прозорість, захист даних і довіру громадян. Документ передбачає досягнення конкретних цифрових цілей: цифровізація ключових публічних послуг, поширення електронної ідентифікації, розвиток цифрових навичок, що потребує системної координації моніторингу їх впровадження у публічному секторі.

В посібнику E-Leaders з управління цифровим урядом (The E-Leaders Handbook on the Governance of Digital Government, OECD, 2021) [180] обґрунтовується необхідність створення цілісної системи електронного урядування на основі принципів відкритості, спільного управління даними, користувацько-орієнтованого дизайну та постійної інституційної адаптації. Рекомендації OECD підкреслюють важливість інтеграції цифрових стратегій з процесами планування та бюджету, формування відповідних організаційних структур (наприклад, digital units або policy labs), а також належного інституційного моніторингу через якісні індикатори, циклічні огляди, міжвідомчу звітність та залучення стейкхолдерів.

*Емпірична обґрунтованість* забезпечується за рахунок поглибленої бази даних: технічних логів, реєстрів, аудиторських звітів та соціологічних досліджень. Згідно з документом OECD «Digital Government Policy Framework» (2020), новітні системи моніторингу вимагають чіткого визначення метрик,

критеріїв якості даних, процедур верифікації та комбінованого використання кількісних і якісних параметрів [181].

*Адаптивність* пов'язується із здатністю системи реагувати на швидкі зміни: появу нових технологічних трендів (як-от штучний інтелект, блокчейн, хмарні та туманні сервіси), оновлення нормативно-правової бази (наприклад, введення в дію Регламенту (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку (eIDAS Dashboard, 2014) [182]; Регламенту (ЄС) про європейське управління даними (Data Governance Act, 2022) [183]; Закону про інтероперабельну Європу (EU Interoperable Europe Act, 2024) [184]; та зміни ролей та організаційних моделей через інституційні реформи тощо.

Відповідно, матриця передбачає:

- комбіноване використання індикаторів: технічних (кількість API, рівень інтеграції), організаційних (спроможність персоналу, внутрішні політики), правових (відповідність стандартам), соціальних (рівень доступності, задоволеність громади) і ефективності (аналітика часу обробки запитів);
- використання різнотипних шкал: кількісних (відсоткові показники), якісних (експертна оцінка), бінарних (наявність/відсутність) та агрегованих індексів (наприклад, індекс цифрової зрілості);
- порівняння результатів з міжнародними трендами (DESI, OECD DGI, EGDI) і локальними стандартами, що створює міцну основу для контекстуалізації оцінювання, встановлення базових ліній, формування траєкторій розвитку та раннього виявлення відхилень;
- періодичний перегляд та оновлення, враховуючи нові технології, норми та загрози (кібербезпеку, digital rights, AI governance), що відповідає концепції циклічного планування (plan-do-check-act) в електронному урядуванні.

Таким чином, окреслена методологія дозволяє розробити матрицю моніторингу, яка передбачає не лише можливість оцінити поточний стан цифрової взаємодії органів, а й формування підґрунтя для стратегічної адаптації, прогнозування ризиків, корекції політики на основі об'єктивних і науково

обґрунтованих даних.

Цей підхід узгоджується з міжнародними методологіями, зокрема OECD Digital Government Index (DGI), який пропонує інтегровану систему оцінювання цифрового розвитку за шістьма вимірами: цифровий за дизайном (digital by design); публічний сектор, що керується даними (data-driven public sector); уряд як платформа (government as a platform); відкритість за замовчуванням (open by default); орієнтованість на користувача (user-driven); проактивність (proactiveness), а також трансверсальними осями моніторингу, політичної волі, імплементації й стратегічного бачення. Методологія DGI підкреслює необхідність поєднання кількісних та якісних індикаторів, а також використання агрегованих індексів для аналітичної оцінки стану цифрової зрілості державних органів [185].

Вказані документи формують рамку розвитку електронного урядування національного рівня як цілісної політики, орієнтованої на ефективність, прозорість, інклюзивність та сталість цифрових сервісів. Такий підхід відповідає сучасним тенденціям електронного урядування, що відображено в міжнародних документах, зокрема рекомендаціях Єврокомісії «Digital Decade» [52], у яких використовується багаторівнева структура показників для оцінки цифрової зрілості держав. Наприклад, згадувана вище «Цифрова декада Європи» визначає чотири основні напрями цифрової трансформації: цифрові навички, інфраструктура, цифровізація бізнесу та цифровізація публічних послуг, які мають бути піддані регулярному моніторингу через відповідні показники тощо. Таким чином, акцентується увага не лише на результатах цифровізації, а й на процесах, що їх супроводжують, включаючи управлінську спроможність, інституційні моделі координації, міжвідомчу взаємодію та відповідність цифрових рішень правовим нормам і етичним стандартам.

Стратегія цифрової трансформації України (затверджена у 2024 р.) [156] проголошує метою побудову сервісної держави, у якій цифрові послуги є безпечними, зручними та доступними для всіх. Згідно з цим документом, цифрова трансформація вимагає постійної оцінки ступеня інтегрованості,

прозорості, ефективності та інноваційності у роботі органів публічної влади. Саме тому формування національної системи моніторингу цифрової взаємодії стає важливою складовою цифрової політики, здатною забезпечити не лише контроль і звітність, а й зворотний зв'язок для адаптації стратегій і підходів.

Як зазначалось вище, окрему роль відіграє індекс розвитку електронного урядування EGDI, запропонований ООН, який є глобальним стандартом для оцінки цифрової зрілості держав. Його структура, що включає індекси онлайн-послуг, людського капіталу та телекомунікативної інфраструктури, демонструє важливість багатовимірної методології, в якій електронне урядування розглядається як результат взаємодії різних компонентів: технологічного, організаційного, освітнього, нормативного тощо.

Всі ці підходи підкреслюють необхідність уніфікованої та водночас гнучкої системи моніторингу, що дозволяє не лише оцінити поточний стан цифрової взаємодії, а й коригувати політику, виявляти системні бар'єри, стимулювати розвиток людського потенціалу та підвищувати якість цифрових рішень. У цьому контексті пропонується матриця моніторингу вбачається дієвим інструментом реалізації принципів *evidence-based policy* (політики, заснованої на доказах) та забезпечення сучасного електронного урядування, що відповідає національним пріоритетам та світовим стандартам.

Розробка матриці моніторингу функціонування механізмів цифрової взаємодії органів публічної влади потребує чітко структурованого підходу до *визначення джерел інформації*. На першому етапі особливого значення набуває ідентифікація таких джерел, які є репрезентативними, достовірними та релевантними до цілей моніторингу. У цьому контексті актуальним є мультиджерельний підхід, що поєднує як формалізовані технічні дані, так і соціальні та поведінкові індикатори.

Провідну роль відіграють офіційні державні інформаційні системи, які надають дані щодо технічного стану цифрових платформ, обсягів обміну інформацією між реєстрами, рівня інтеграції та сумісності міжвідомчих ІКТ-систем. Однак цього недостатньо для отримання повної картини. Важливим

джерелом є звіти незалежних аудитів, зокрема у сфері кібербезпеки, які дозволяють верифікувати відповідність цифрової інфраструктури міжнародним стандартам, таким як ISO/IEC 27001. Особливої актуальності така практика набуває в умовах зростання кіберзагроз і вимог до захищеності персональних даних. У цьому сенсі нормативно-правова база ЄС, зокрема Регламент (ЄС, Євратом) 2023/2841, визначає аудит кібербезпеки як базовий інструмент підвищення надійності публічного управління. Впровадження аналогічних механізмів в Україні є необхідною умовою наближення до європейських стандартів захисту даних та надійності цифрових систем [186].

Значну аналітичну цінність мають опитування користувачів цифрових послуг. У цьому аспекті важливо враховувати суб'єктивну оцінку зручності, зрозумілості та доступності сервісів та рівень довіри до цифрових інструментів. Згідно з регулярними звітами ООН у межах UN E-Government Survey, саме систематичне врахування зворотного зв'язку від громадян дозволяє державам ефективно вдосконалювати цифрову взаємодію [4; 109; 172]. Залучення користувача до процесу моніторингу сприяє посиленню прозорості, підзвітності та адаптивності публічних цифрових послуг.

Ці тези підтверджуються в дослідженнях провідних науковців. Зокрема, Н. Едельманн, Н. Гауг та І. Мергель у статті «Digital Transformation in the Public Sector» (2023) акцентують увагу на необхідності інтегрувати адміністративні, поведінкові та технологічні дані в єдиний аналітичний простір. Авторки стверджують, що ефективна оцінка цифрової трансформації можлива лише за умови виходу за межі вузько технократичного підходу до цифровізації, коли оцінюються не лише «залізо» й «код», а й соціокультурні передумови змін, включно з цифровою грамотністю та організаційною культурою [187].

Цю позицію розвиває також М.Ліпс у роботі «Digital Transformation in the Public Sector: Collaborating for Digital Transformation» (2024). Дослідниця акцентує на «людиноцентричному» вимірі цифрового розвитку, підкреслюючи, що громадяни мають виступати не просто споживачами послуг, а повноцінними учасниками процесу цифрового моніторингу. Саме такий підхід, за М.Ліпс,

створює основу для формування більш адаптивних, справедливих і соціально вмотивованих цифрових політик. Її ідеї гармонізуються з концепцією «спільного створення» цифрових послуг (co-creation), що активно просувається у європейських дослідженнях електронного урядування [188].

Крім того, джерелами даних для формування матриці моніторингу можуть бути внутрішні документи органів публічної влади: регламенти, політики, посадові інструкції, навчальні плани. Вони свідчать про інституційну готовність до цифрових змін і наявність у структурі органу механізмів підтримки цифрової зрілості. Автоматизовані моніторингові системи, що забезпечують збір даних у реальному часі (наприклад, щодо часу відгуку сервісу, кількості відмов, навантаження на сервери тощо), також є незамінним джерелом у процесі технічної оцінки ефективності.

Таким чином, наукові та практичні підходи до визначення джерел даних для цифрового моніторингу все більше тяжіють до інтегративної моделі, яка поєднує технічні, соціальні, нормативні та інституційні аспекти. Це забезпечує глибину аналітики, дає змогу виявляти не лише симптоми, але й причини дисфункцій цифрової взаємодії, та створює умови для системного управління цифровою трансформацією в публічному секторі.

*Визначення індикаторів* є основним етапом побудови матриці моніторингу функціонування цифрових механізмів у публічному управлінні. Індикатори виступають аналітичними змінними, які дозволяють системно оцінити стан, динаміку й ефективність цифрової взаємодії органів влади. При цьому критично важливими є такі характеристики індикаторів, як релевантність, вимірюваність, надійність та порівнюваність, що дає змогу здійснювати не лише внутрішній аналіз, а й міжінституційні та міжрегіональні зіставлення.

Світова практика демонструє переваги багатовекторного (мультидименсійного) підходу до побудови індикативної системи. Такий підхід враховує не лише технічні характеристики, а й інституційні, управлінські, соціальні та нормативно-правові аспекти цифрової трансформації. У цьому контексті показовою є методологія Світового банку, представлена у звіті

GovTech Maturity Index: The State of Public Sector Digital Transformation (2021), яка пропонує п'ятирівневу модель індикаторів. До неї відносять:

- стратегію цифрової трансформації, що оцінює наявність візії, цілей і планів дій;
- інституційну базу, яка включає політики, регуляції, організаційні структури та кадровий потенціал;
- цифрову інфраструктуру (наявність інтегрованих платформ, кіберзахист, інтероперабельність);
- цифрові послуги, оцінка їх доступності, якості, масштабованості;
- залучення користувачів, що передбачає участь громадян у створенні цифрових рішень та надання зворотного зв'язку.

Особливо цінним у цій моделі є інтеграція організаційних і поведінкових вимірів, що дозволяє переходити від аналізу «зовнішніх результатів» до розуміння внутрішньої спроможності публічних інституцій до цифрових змін [189].

Іншу вагому концептуальну рамку пропонує Організація економічного співробітництва та розвитку (ОЕСР), яка у Digital Government Index (2023) розширює акцент з технічних аспектів цифровізації до більш управлінсько-орієнтованих категорій. Зокрема, пропонується оцінка індикаторів відкритості даних, прозорості прийняття рішень, впровадження інновацій, рівня організаційної гнучкості та здатності до стійкого цифрового розвитку. У фокусі не просто ефективність роботи ІТ-систем, а трансформаційна здатність інституцій на основі використання цифрових технологій [190]. Цей підхід дозволяє осмислювати цифровізацію як інструмент управління змінами, а не лише як набір ІТ-рішень.

Європейська комісія у рамках ініціативи Digital Government Benchmark (2024) [191] також активно просуває багатовекторну модель оцінювання. Запропонована структура охоплює індикатори чотирьох основних блоків:

- доступність цифрових сервісів (усунення бар'єрів, охоплення вразливих груп);

- інтеграція послуг (ступінь з'єднаності між платформами, рівень автоматизації);
- безпека даних і систем (відповідність стандартам, впровадження засобів контролю);
- користувацький досвід (юзабіліті, інтуїтивність, якість обслуговування).

Перевагою цього підходу є можливість порівняння рівня цифрового розвитку в межах ЄС, зокрема на міждержавному рівні, а також його адаптація для оцінювання цифрової зрілості в межах окремих регіонів, що є особливо релевантним для України в умовах територіально неоднорідного розвитку цифрової інфраструктури.

Вищезазначене дозволяє дійти висновку, що сучасні системи індикаторів моніторингу електронного урядування мають переходити від одновимірного аналізу технічної ефективності до багатовимірного аналізу організаційної спроможності, користувацької орієнтованості та управлінської інноваційності. Такий підхід дозволяє не лише відстежувати прогрес, але й виявляти вразливі місця, встановлювати стратегічні пріоритети й адаптувати політику цифровізації до потреб конкретного адміністративного контексту. Для України, яка прагне до інтеграції в Європейський цифровий простір, адаптація цих підходів є важливою умовою забезпечення системності та стійкості цифрової трансформації публічного сектору.

Для ефективного оцінювання функціонування механізмів цифрової взаємодії в публічному управлінні України важливо не лише адаптувати міжнародні підходи, а й розробити таку систему індикаторів, яка б враховувала національні контексти, специфіку інституційного розвитку та нерівномірність цифровізації у регіонах. В українській практиці доцільним є виокремлення п'яти основних груп індикаторів: технічних, організаційних, юридичних, соціальних та індикаторів ефективності.

Технічні індикатори охоплюють параметри, що безпосередньо характеризують стан цифрової інфраструктури: кількість інтегрованих реєстрів,

доступність API, частота технічних збоїв, наявність сертифікатів відповідності кібербезпеки тощо. Ці індикатори є базисом для оцінки технологічної спроможності системи.

Організаційні індикатори фокусуються на внутрішній готовності інституцій до цифрової трансформації: наявність внутрішніх політик управління ІТ, рівень цифрових компетентностей працівників, адаптивність управлінських структур. Цей блок дозволяє оцінити, наскільки організація є стійкою до цифрових змін і чи здатна вона ефективно інтегрувати нові технології у свою діяльність.

Юридичні індикатори передбачають вимірювання відповідності правовій базі у сфері цифровізації, наявності внутрішніх регламентів цифрової взаємодії, а також рівня імплементації європейських директив. Це важливо для оцінювання правової спроможності цифрового управління.

Соціальні індикатори забезпечують вимірювання користувацької складової: задоволеності громадян, рівня інклюзивності цифрових послуг, динаміки звернень і скарг. Такий підхід посилює соціоцентричний вектор цифровізації, виводячи людину в центр управлінського процесу.

Індикатори ефективності – це аналітичні змінні, які демонструють результативність цифрових сервісів (наприклад, середній час обробки запитів, кількість доступних сервісів, рівень прозорості тощо). Вони є критичними для оцінювання досягнутих результатів і визначення зони для вдосконалення.

У звіті Національного інституту стратегічних досліджень (2025), у якому проаналізовано цифрову трансформацію економіки України, запропоновано саме таку функціональну структуру індикаторів. Її застосування у пропонуваній матриці дозволяє створити системну та цілісну модель оцінювання цифрової зрілості публічного управління. Цей підхід демонструє високу адаптивність та логіку взаємопов'язаного аналізу окремих аспектів цифровізації [192].

Також емпіричну базу для моніторингу формує Звіт Мінцифри України (2024), у якому міститься деталізована інформація про розвиток цифрової інфраструктури в регіонах, рівень цифрової освіти публічних службовців, а

також темпи впровадження нових сервісів [193]. Така інформація дозволяє не лише оцінити поточний стан, а й виявити регіональні диспропорції та ефективність реалізації цифрових стратегій на місцевому рівні.

*Оцінювання кожного індикатора* відбувається із застосуванням відповідних шкал. Залежно від природи даних, застосовуються чотири основні типи шкал:

- кількісні шкали базуються на об'єктивних числових значеннях (наприклад, відсоток інтегрованих систем, тривалість обробки звернень), що забезпечує точність, відтворюваність і можливість міжорганізаційного порівняння;

- якісні шкали дозволяють враховувати поведінкові та культурні фактори (наприклад, рівень цифрової культури чи дотримання етичних норм), які складно виразити у цифрах, але які критично впливають на успіх цифрової трансформації;

- бінарні шкали є зручними для попереднього скринінгу (наявність/відсутність політик, інструментів кіберзахисту, регламентів), що дозволяє швидко ідентифікувати прогалини;

- індекси та агреговані показники, як-от Digital Maturity Index, інтегрують декілька змінних у комплексну оцінку рівня цифрової зрілості.

Дослідження компанії Gartner (2024) підкреслює ефективність поєднання кількісних і якісних шкал, акцентуючи на гібридному вимірі цифрової зрілості на основі аналітики, що ґрунтується не лише на технічних метриках, а й на управлінських практиках та поведінкових характеристиках організацій [194].

У роботі С.Гадалай «Cybersecurity Assessments» доводить ефективність використання скринінгу кібербезпеки, що дозволяє швидко ідентифікувати критичні проблеми та вжити своєчасних управлінських заходів та є особливо важливий у контексті забезпечення стійкості цифрової інфраструктури до зовнішніх впливів [195].

Окремо слід відзначити показник Digital Maturity Index, запропонований компанією Deloitte, який застосовується в міжнародній практиці як комплексний

інструмент для оцінювання цифрової зрілості в публічному секторі [196]. Цей індекс охоплює технологічні, кадрові та інституційні компоненти цифрової трансформації, забезпечуючи не лише вимірювання поточного стану, а й діагностику готовності до майбутніх змін.

Практична реалізація зазначеної методології можлива шляхом побудови багатовимірної матриці, у якій індикатори співвідносяться з відповідними напрямками цифрової взаємодії. Матриця дозволяє візуалізувати поточний стан функціонування механізмів, ідентифікувати зони ризику, виявити «вузькі місця» у цифровій інфраструктурі або організаційній спроможності. Прикладом подібного інструменту в українській практиці є «Матриця реформ 2025», яка акумулює ключові цілі, заходи, індикатори та очікувані результати реалізації реформ у форматі інтерактивної аналітичної системи та дозволяє залученим сторонам оперативно виявляти проблемні зони та оцінювати прогрес [197].

Індекси ООН, зокрема Індекс розвитку електронного уряду (E-Government Development Index, EGDI) та Індекс онлайн-сервісів (Online Service Index, OSI), є складовою частиною Індексу розвитку електронного урядування, розробленого ООН. Він оцінює обсяг і якість онлайн-послуг, що надаються органами публічної влади, на основі даних, зібраних за допомогою незалежної анкети Online Service Questionnaire (OSQ) [198]. Ці індекси є основними міжнародними інструментами для системного вимірювання рівня цифрової зрілості держав у сфері публічного управління. Їх значущість полягає у можливості інтегрувати кількісні й якісні параметри в уніфіковану аналітичну систему, що дозволяє здійснювати глобальні порівняння та національне планування цифрових політик.

EGDI є композитним показником, що поєднує три складові:

Online Service Index (OSI) – рівень надання цифрових публічних послуг через державні вебресурси;

Telecommunication Infrastructure Index (TII) – ступінь розвитку телекомунікативної інфраструктури (кількість інтернет-користувачів, мобільних підписок, широкосмугових з'єднань тощо);

Human Capital Index (HCI) – освітній рівень населення, що включає

показники грамотності, охоплення вищою та середньою освітою. Цей індекс демонструє багатовекторний підхід до моніторингу цифровізації, у якому враховуються не лише технічні та інфраструктурні аспекти, а й соціальні передумови ефективного впровадження електронного врядування. Такий підхід підтримує логіку цифрової рівності й інклюзії [172].

OSI є підіндексом EGDI, але окремо використовується як важливий інструмент оцінки цифрових послуг, що надаються урядами. Він базується на оцінці доступності електронних сервісів (від інформаційних до інтерактивних і транзакційних); ступеня персоналізації послуг; мовної доступності; доступу для вразливих груп населення; наявності функцій зворотного зв'язку; використання відкритих даних та e-participation інструментів. Цей індекс ілюструє, як якісні параметри цифрового досвіду громадян: зручність, доступність, персоналізація можуть бути переведені в формалізовані критерії оцінки, що підлягають моніторингу. При цьому OSI враховує змістовну складову цифрового урядування, підкреслюючи не лише наявність сервісу, а його ефективність та інклюзивність.

Інтеграція кількісних (інфраструктура, охоплення, цифрова грамотність) та якісних (досвід користувача, відкритість, інклюзивність) параметрів в індексах ООН відповідає концепції «комплексної цифрової трансформації», яка все більше реалізується і в українському підході до моніторингу. До прикладу, національні звіти Мінцифри та дані платформи «Дія» також починають враховувати не лише технічні характеристики, а й зворотний зв'язок громадян.

Україна, яка вже має позитивну динаміку в EGDI (наприклад, за даними Мінцифри 2024 року Україна посіла 5-те місце за індексом онлайн-сервісів у глобальному рейтингу ООН) [199], може використовувати методологію цих індексів як еталонну рамку для внутрішньої побудови системи моніторингу. Зокрема, EGDI може слугувати референтною моделлю для створення національного індексу цифрової зрілості на рівні регіонів чи окремих органів влади. Методологія ООН демонструє, що ефективна цифрова трансформація вимірюється не лише кількістю впроваджених ІТ-рішень, а ступенем їхньої

інтеграції в соціальні, освітні та управлінські процеси. Саме така логіка покладена в основу пропонованої матриці моніторингу цифрової взаємодії органів публічної влади (табл 3.2.), яка комбінує технічну оцінку з соціальною та інституційною аналітикою.

Таблиця 3.3

Матриця моніторингу функціонування механізмів цифрової взаємодії органів публічної влади

Сфера оцінювання	Група індикаторів/ Показники	Джерела даних	Тип шкали оцінювання	Тип розрахунку оцінювання
<b>Технічна взаємодія</b>	<i>Технічні:</i> Кількість інтегрованих систем Наявність API Частота технічних збоїв	Державні ІС, реєстри, СЕД Реєстри інтеграції, технічні логи	Кількісна / Бінарна	Абсолютна кількість, частота на одиницю часу, бінарна наявність (0/1)
<b>Інформаційна сумісність</b>	<i>Юридичні, технічні:</i> Відповідність даних стандартам (X-Road, XML, RDF) Виконання вимог законодавства	Акти технічної перевірки Юридичні експертизи	Якісна / Бінарна	Відсоток відповідності, ступінь відповідності за шкалою, наявність/ відсутність
<b>Організаційна спроможність</b>	<i>Організаційні:</i> Частка працівників, що пройшли цифрове навчання Наявність політик цифрового управління	Внутрішні документи органів влади HR-звіти, навчальні програми	Кількісна / Якісна	Відсоток від загальної кількості, оцінка за шкалою (наприклад, 0-5)
<b>Правове забезпечення</b>	<i>Юридичні:</i> Наявність внутрішніх регламентів цифрової взаємодії Ступінь імплементації директив ЄС	Відомчі нормативні акти Оцінки відповідності міжнародним стандартам	Бінарна / Якісна	Бінарна (є/немає), відсоток імплементованих положень

## Продовження таблиці 3.3

<b>Кібер-безпека</b>	<i>Технічні, юридичні:</i> Кількість сертифікатів відповідності (ISO/IEC 27001) Виявлені інциденти	Аудити кібербезпеки Звіти Служби спеціального зв'язку та захисту інформації	Кількісна / Бінарна	Абсолютна кількість, відсоток сертифікованих систем, частота інцидентів на рік
<b>Соціальна інклюзія</b>	<i>Соціальні:</i> Рівень задоволеності користувачів Доступність сервісів для маломобільних груп	Опитування громадян Звіти Уповноваженого з прав людини	Якісна / Кількісна	Бал за шкалою задоволеності (0-10), частка адаптованих сервісів у загальній кількості
<b>Ефективність послуг</b>	<i>Ефективність:</i> Середній час обробки запитів Кількість електронних послуг, що надаються	Реєстри звернень Аналітика фронт-офісів Системи онлайн-запису	Кількісна	Середнє значення в секундах/хвилинах, абсолютна кількість або кількість на 1000 осіб
<b>Відкритість і прозорість</b>	<i>Соціальні, ефективність:</i> Наявність відкритих даних Доступність інформації на порталах органів влади	Єдиний портал відкритих даних Сайти органів публічної влади	Бінарна / Кількісна	Відсоток від оприлюднених даних, бінарна оцінка наявності розділів (0/1), обсяг даних у МБ
<b>Загальна цифрова зрілість</b>	<i>Агреговані індекси:</i> Композитний індекс цифрової зрілості (на основі сумарної оцінки за всіма напрямками)	Агреговані дані з усіх попередніх джерел	Індекс / Зведений бал	Зважене середнє, нормалізований бал (наприклад, шкала 0-100), інтегральна оцінка

Джерело: складено автором

Запропонована матриця моніторингу функціонування механізмів цифрової взаємодії органів публічної влади є інструментом, що поєднує міждисциплінарний підхід до оцінювання цифрових процесів у публічному

секторі. Вона охоплює широкий спектр сфер: технічну, інформаційну, організаційну, правову, соціальну, і забезпечує системну оцінку як внутрішньої спроможності органів влади, так і зовнішніх проявів ефективності цифрових сервісів.

Визначальною особливістю матриці є її багаторівнева структура, що базується на:

- різнорівневих шкалах оцінювання (кількісних, якісних, бінарних, індексних),
- комплексному залученні джерел даних (офіційні реєстри, нормативні акти, внутрішні звіти, результати опитувань, аналітика фронт-офісів тощо),
- багатовекторному підборі індикаторів, які відповідають як технічним характеристикам цифрової взаємодії, так і соціальній цінності цифрових сервісів.

У складі матриці окремо зазначено тип розрахунку кожного показника, що забезпечує уніфікованість та порівнюваність результатів моніторингу на різних рівнях. Такий підхід дозволяє точно визначати формат обчислення залежно від природи індикатора. Зокрема, застосовуються абсолютні величини (наприклад, кількість електронних послуг, зареєстрованих інцидентів або сертифікованих систем); відносні значення (відсоток у загальному обсязі, частка від нормативного орієнтира); частотні характеристики (наприклад, кількість технічних збоїв на одиницю часу); бальна оцінка за шкалою (рівень задоволеності користувачів, цифрова культура персоналу); агреговані індекси (інтегральна оцінка цифрової зрілості за сукупністю параметрів).

Це забезпечує гнучкість у використанні матриці як інструменту порівняльного аналізу, дає можливість адаптувати її до контексту кожної конкретної організації або регіону, а також дозволяє використовувати її результати як в оперативному, так і в стратегічному плануванні.

Матриця є адаптивною до змін цифрового середовища, її структура дозволяє оперативно оновлювати індикатори та джерела даних у разі появи нових технологічних викликів, змін у нормативно-правовій базі або пріоритетах державної цифрової політики. Це відповідає положенням Концепції розвитку

електронного урядування в Україні, в якій моніторинг визначено як ключовий інструмент стратегічного управління цифровими реформами.

Вважаємо, що впровадження матриці моніторингу функціонування механізмів цифрової взаємодії як вітчизняної оціночної методики є важливим кроком на шляху до інституціоналізації системного аналізу цифрових трансформацій у публічному управлінні. Вказане дозволяє не лише забезпечити об'єктивне вимірювання ефективності цифрових процесів, але й сформувати підґрунтя для прийняття обґрунтованих управлінських рішень, спрямованих на підвищення прозорості, відкритості, адаптивності та стійкості систем електронного урядування. Впровадження матриці сприятиме формуванню цілісної аналітичної культури в органах публічної влади, що дозволить більш гнучко реагувати на виклики цифрової епохи, покращити якість державних сервісів та зміцнити довіру громадян до публічних інституцій.

### **3.3. Пропозиції та рекомендації щодо пріоритетних напрямів удосконалення механізмів цифрової взаємодії органів публічної влади для ефективного розвитку електронного урядування**

У попередніх розділах дисертаційного дослідження було здійснено системне теоретико-методологічне обґрунтування цифрової взаємодії в системі публічного управління, розкрито еволюцію ключових понять і підходів до електронного урядування, проаналізовано зарубіжні практики впровадження інтегрованості інформаційних систем, а також виявлено актуальні виклики для цифрової взаємодії в Україні в контексті безпеки, довіри та ефективності.

Водночас результати аналізу засвідчують, що попри наявні зрушення у сфері цифровізації, в Україні ще не створено повноцінної інституційно-координованої системи цифрової взаємодії органів публічної влади, що функціонує на засадах технологічної інтеграції, нормативної узгодженості та кадрової спроможності. Потреба в системному оновленні управлінських практик, з урахуванням динаміки цифрових трансформацій та світових

стандартів електронного урядування, зумовлює необхідність формулювання практико-орієнтованих рекомендацій. Відтак, постає завдання конкретизації стратегічних і тактичних кроків, що сприятимуть підвищенню ефективності цифрової взаємодії в системі органів публічної влади. Це особливо актуально в умовах посилення ролі цифрових технологій у формуванні відкритого та інклюзивного управління, що відповідає суспільним очікуванням і європейським інтеграційним орієнтирам України.

Удосконалення механізмів цифрової взаємодії органів публічної влади потребує системного підходу, який охоплює одночасно нормативну, організаційну та технологічну складові. Вважаємо, що зміни на кожному з рівнів мають бути взаємопов'язаними, інтегрованими в єдину державну політику цифрової трансформації та відповідати міжнародним зобов'язанням України та внутрішнім управлінським реаліям.

*Національний рівень.* Одним із головних викликів цифрової взаємодії в Україні на національному рівні є фрагментарність нормативно-правового забезпечення. Незважаючи на ухвалення базових законів, таких як Закон України «Про публічні електронні реєстри» (2022) [200] та Закон «Про захист персональних даних» [83], нормативна база залишається розпорошеною, а положення щодо інтероперабельності інформаційних систем органів влади — недостатньо деталізованими. Як свідчать аналітичні матеріали платформи Interoperable Europe (European Commission, IOPEU Monitoring), Україні бракує цілісної рамки управління міжвідомчим обміном даними, що ускладнює ефективне функціонування цифрових сервісів [201].

У цьому контексті особливо актуальним є досвід Європейського Союзу, закріплений у Європейській рамці інтероперабельності (EIF) та нещодавно запропонованому «Регламенті про взаємодію в ЄС» (Interoperable Europe Act). Практика Європейського Союзу показує, що ключовим кроком до забезпечення ефективної цифрової взаємодії є розробка та впровадження Національної системи управління інтероперабельністю, яка базується на принципах, закладених в Європейській рамці інтероперабельності (EIF).

Наразі Україна використовує платформу «Трембіта» (аналог естонської X-Road), однак ця технологія залишається технічним інструментом, позбавленим достатньої інституційної координації. У зв'язку з цим доцільним є створення міжвідомчого координаційного органу на зразок Interoperable Europe Board (постійного координаційного органу, що визначає стандарти, розробляє спільні рішення і забезпечує обмін кращими практиками), що діє в Європарламенті (звіт Європарламенту A9-0254/2023). Його повноваження мають включати визначення технічних стандартів, забезпечення правової уніфікації цифрової взаємодії та координацію процесів впровадження на всіх рівнях влади [202].

Адаптація цієї моделі до українського контексту вимагає не лише інституціалізацію керівного органу з управління інтероперабельністю, але й формування єдиного правового поля, що забезпечує уніфікацію цифрової взаємодії на всіх рівнях влади. Це дозволить запобігти дублюванню функцій, підвищити прозорість обробки даних і створити умови для підзвітності цифрових трансформацій.

*Організаційний рівень.* На організаційному рівні ключовою передумовою сталого цифрового розвитку є підвищення внутрішньої керованості цифровими процесами в органах публічної влади регіонального та місцевого рівнів. Відсутність стандартизованих підходів до внутрішнього аудиту цифрових операцій призводить до втрат ефективності, ризиків дублювання даних і слабкої ідентифікації вузьких місць у сервісах.

Практика компаній приватного сектору (наприклад, Deloitte або WestRock) свідчить про ефективність використання внутрішнього цифрового аудиту як інструменту стратегічного планування цифрової трансформації. Як засвідчено у кейсі компанії WestRock, описаному в аналітичному огляді Deloitte у CIO Journal, використання генеративного ШІ дозволило значно підвищити ефективність контролю цифрових процесів. Запровадження подібної практики в українських ЦОВВ та ОМС сприятиме виявленню слабких місць, ризиків дублювання функцій та оптимізації внутрішніх процесів [203].

Запровадження подібної моделі на рівні публічних інституцій в Україні має здійснюватися за допомогою формування спеціалізованих *Digital Units* або *Цифрових офісів*. Відповідно до дослідження Paolo Ciancarini та співавторів (2023), такі офіси мають здійснювати супровід цифрових трансформацій, забезпечувати технічний бенчмаркінг та підтримувати цифрову грамотність персоналу. Їх функціонування потребує інституціонального закріплення ролі CDTO (Chief Digital Transformation Officer), що відповідає за стратегію цифрових змін в органі влади [204].

*Технологічний рівень.* На цьому рівні передбачено впровадження інноваційних ІКТ-рішень, які забезпечують інтелектуальне управління даними, масштабованість сервісів та безперервність надання цифрових послуг. У першу чергу йдеться про інтеграцію технологій штучного інтелекту, хмарних платформ і обробки великих даних (Big Data).

Сучасні підходи до цифрової трансформації публічного управління дедалі частіше передбачають інтеграцію інструментів штучного інтелекту (ШІ), що здатні забезпечити новий рівень ефективності адміністративних процесів. Застосування ШІ у публічному секторі охоплює, зокрема, автоматизовану попередню обробку звернень громадян, класифікацію проблем за типологією, виявлення аномалій у транзакційних потоках (зокрема у сфері публічних фінансів чи закупівель), а також підтримку ухвалення управлінських рішень шляхом аналізу великих обсягів даних. Такі технології формують основу так званого data-driven governance-управління, орієнтованого на дані, що суттєво розширює аналітичні спроможності органів публічної влади [205].

Однак, впровадження ШІ у сфері публічного управління потребує дотримання низки етичних та нормативних принципів. Зокрема, йдеться про забезпечення прозорості алгоритмічних рішень, уникнення дискримінаційних практик та гарантування пояснюваності (explainability) прийнятих рішень. У цьому контексті особливого значення набуває Європейський підхід до етичного ШІ, зокрема Рекомендації Вищої експертної групи з питань ШІ при Єврокомісії (2019), що можуть бути адаптовані до українських реалій як орієнтир для

розробки національної етики цифрових систем [206].

Інфраструктурною основою впровадження інтелектуальних сервісів є хмарні технології, які дозволяють масштабовано зберігати, обробляти й передавати дані у межах захищених цифрових середовищ. Закон України «Про хмарні послуги» визначає пріоритетність застосування хмарної архітектури у діяльності органів державної влади, органів місцевого самоврядування, державних підприємств та суб'єктів, що надають публічні послуги [207].

Принцип «Cloud-First», закріплений у цьому законі, передбачає поступову відмову від фрагментованих (локальних) ІТ-інфраструктур на користь інтегрованих хмарних рішень. Застосування принципу «Cloud-First» сприяє зменшенню бюджетних витрат на створення й утримання ІТ-інфраструктури, підвищенню надійності цифрових сервісів, забезпеченню резервного копіювання та гнучкому управлінню навантаженнями. Для малих громад або територіальних громад з обмеженими ІТ-ресурсами це відкриває можливість інтегруватися в єдиний цифровий простір держави без потреби в дорогому локальному обладнанні, тим самим усуваючи цифрову нерівність і розширюючи доступ до публічних сервісів. У перспективі це формує передумови для створення національного хмарного середовища, інтегрованого з реєстрами та платформами електронного урядування.

Закон також визначає основні нормативні засади функціонування хмарної інфраструктури, включаючи вимоги до безпеки, обов'язкове зберігання даних на території України, механізми контролю доступу до інформації, рівні відповідальності хмарних провайдерів, а також процедурні правила переходу органів публічної влади до хмарних сервісів. Головними технічними орієнтирами виступають міжнародні стандарти інформаційної безпеки, зокрема ISO/IEC 27001, 27017 та 27018, які забезпечують відповідність систем захисту персональних і службових даних сучасним вимогам.

Особливу цінність у контексті розвитку цифрової взаємодії становить застосування технологій обробки великих даних (Big Data) у межах державних платформ, зокрема платформи «Трембіта». Ця система електронної взаємодії

державних електронних інформаційних ресурсів, створена на основі естонської технології X-Road, дозволяє забезпечити безпечний обмін даними між різними реєстрами та базами даних органів публічної влади без дублювання інформації та без її фізичного переміщення. Завдяки своїй архітектурі, «Трембіта» підтримує побудову аналітичних дашбордів, які інтегрують дані з різнорідних джерел - державних реєстрів, геоінформаційних систем, фінансових звітів, соціальних платформ тощо. Це відкриває широкі можливості для застосування Big Data у публічному управлінні. Зокрема, йдеться про:

- прогнозу аналітику (формування моделей, що передбачають зміни в запитах громадян, навантаження на ЦНАПи чи соціальні служби);
- ризик-менеджмент (оперативне виявлення аномалій у системі надання послуг, зокрема у публічних закупівлях, податкових взаємодіях або видачі дозволів);
- антикорупційний моніторинг (аналіз транзакцій, поведінкових патернів, повторюваних зв'язків між суб'єктами публічного сектору);
- персоналізацію послуг (адаптацію цифрових сервісів до потреб окремих категорій громадян, урахування індивідуальних траєкторій життєвих подій у форматі «життєвих ситуацій») [208].

Згідно з аналітичними оглядами, оприлюдненими на порталі реформ [uareforms.org](http://uareforms.org) [209], використання Big Data в межах платформи «Трембіта» уже дозволяє формувати дашборди для обласних державних адміністрацій та ЦОВВ, які включають індикатори доступності послуг, часу обробки звернень, кількості відмов, що надає керівництву можливість оперативно реагувати на управлінські виклики.

Таким чином, аналітичний потенціал Big Data у публічному секторі є не лише інструментом ефективності, а й основою для побудови проактивного, адаптивного публічного управління, де рішення приймаються не на основі припущень, а на основі даних. У перспективі це сприятиме зміцненню довіри громадян до цифрової держави та підвищенню її результативності.

Реалізація запропонованих механізмів цифрової взаємодії органів

публічної влади передбачає не лише комплексне інституційне та технологічне оновлення, а й усвідомлення потенційних ризиків, що можуть ускладнити або навіть нівелювати очікувані ефекти цифрової трансформації. У цьому контексті доцільно розглядати ризики також в міжрівневій перспективі - на національному, організаційному та технологічному рівнях, кожен з яких має власну специфіку загроз.

На національному рівні центральним органом, відповідальним за цифрову трансформацію, є Міністерство цифрової трансформації України, створене відповідно до Постанови КМУ №856 від 18 вересня 2019 року [210].

Згідно з положенням, міністерство уповноважене формувати та реалізовувати державну політику в таких сферах, як цифровізація, розвиток електронних сервісів, інформаційне суспільство, цифрові права громадян тощо. Міністерство також визначено відповідальним за координацію впровадження електронної взаємодії між державними інформаційними ресурсами.

Водночас, попри стратегічний мандат, функціональні повноваження Міністерства не охоплюють повного спектру регламентації інтероперабельності в її європейському розумінні. Зокрема, Мінцифри не здійснює затвердження обов'язкових технічних стандартів цифрової взаємодії, не має повноважень із санкціонування відхилення від міжвідомчих протоколів і не володіє інструментами нагляду за станом інтеграції цифрових реєстрів усіх ЦОВВ. Це створює умови, за яких органи виконавчої влади, особливо на центральному рівні, часто реалізують цифрові ініціативи у власному форматі, без належної уніфікації з базовими державними платформами.

Порівняльний аналіз із європейською моделлю демонструє, що в Європейському Союзі для забезпечення інтегрованості цифрового простору публічної влади створено окремий орган – Interoperable Europe Board. Цей орган функціонує на підставі Regulation on Interoperable Europe (звіт A9-0254/2023) Європарламент, 2023 [211] та має мандат на методичне, технічне й координаційне забезпечення сумісності цифрових систем у країнах-членах. Його рішення спрямовані на інтеграцію цифрових стандартів у національні стратегії,

розробку інтероперабельних моделей сервісів, управління ризиками та створення спільної бази рішень.

Варто наголосити, що Interoperable Europe Board не є міністерством чи урядовим органом окремої держави-члена, а наднаціональним координаційним органом у системі Європейської Комісії. Проте його функціональне призначення – управління процесами міжвідомчої інтероперабельності, дозволяє здійснити аналітичне порівняння з відповідними повноваженнями національних структур, зокрема Міністерства цифрової трансформації України. Таке зіставлення має не ієрархічний, а функціональний характер і спрямоване на виявлення інституційних прогалин та потенціалу адаптації європейського досвіду (табл. 3.4).

Таблиця 3.4

Виявлення інституційних прогалин та потенціалу адаптації європейського досвіду Мінцифри (Україна) та Interoperable Europe Board (ЄС)

<b>Критерій</b>	<b>Міністерство цифрової трансформації України</b>	<b>Interoperable Europe Board (ЄС)</b>
<b>Статус</b>	Центральний орган виконавчої влади, створений згідно з постановою КМУ	Колегіальний координаційний орган при Європейській Комісії
<b>Основна місія</b>	Політика цифровізації, розвиток е-послуг, електронного урядування	Забезпечення інтероперабельності цифрових систем держав-членів ЄС
<b>Функції щодо інтероперабельності</b>	Формулювання загальної політики, без повноважень обов'язкової стандартизації	Розробка технічних і організаційних стандартів, координація реалізації
<b>Рівень зобов'язань і впливу</b>	Рекомендаційний характер, без права санкціонування чи регламентації	Високий рівень координаційного впливу, інтеграція у бюджетне та проектне планування ЄС
<b>Технічна компетенція</b>	Наявність профільних департаментів у ЦОВВ без централізованої технічної агенції	Працює у взаємодії з DG DIGIT, має доступ до технічних пілотів, інструментів, експертизи

## Продовження таблиці 3.4

<b>Механізми реалізації</b>	Платформи «Дія», «Трембіта», державні проекти цифровізації	Common Interoperability Toolbox, керівні настанови, методична підтримка
<b>Регламентация взаємодії між ЦОВВ</b>	Відсутність обов'язкових протоколів інтеграції національних реєстрів	Оцінка проектів на предмет інтероперабельності, обов'язкові процедури узгодження
<b>Інституційна підзвітність</b>	Підпорядкування КМУ, з обмеженою участю у прийнятті рішень інших ЦОВВ	Взаємодія з Єврокомісією, рекомендації інтегруються в регіональні цифрові стратегії

Джерело: складено автором

Отже, відсутність інституалізованого органу на кшталт Interoperable Europe Board (або брак наділених повноважень Мінцифри з функціями методичного, технічного та моніторингового управління цифровою сумісністю), залишається структурною вразливістю. Як зазначено у звіті Європарламенту А9-0254/2023, саме такі органи забезпечують комплексне управління інтероперабельністю на європейському рівні: від визначення спільних стандартів до практичної підтримки інтеграційних проектів.

На організаційному рівні цифровізації публічної влади критичною проблемою є дефіцит фахівців, здатних підтримувати, розвивати та безпечно експлуатувати цифрову інфраструктуру. Дані міжнародних досліджень свідчать про те, що понад 70 % органів публічної влади в Європі відчувають нестачу цифрових компетенцій серед персоналу.

Очевидно, що ефективна цифрова трансформація ґрунтується на інституціоналізації цифрових офісів та впровадженні посади Chief Digital Transformation Officer (CDTO), заступника керівника з цифровізації, який виконує функції стратегічного цифрового лідера, відповідального за координацію та реалізацію цифрових ініціатив в органах влади. Діяльність CDTO виходить за межі суто технічного супроводу, охоплюючи реінжиніринг застарілих управлінських моделей та формування нової цифрової культури

всередині державних структур.

В Україні роль CDTO все більше визнається як на рівні центральних органів виконавчої влади, так і в територіальних громадах, де цифрові лідери відіграють важливу роль у локальній цифровій трансформації, підвищенні цифрової грамотності працівників та інтеграції сучасних технологій у адміністративні процеси [212]. Водночас, незважаючи на широке впровадження посад CDTO, ефективність їх діяльності значною мірою стримується комплексом організаційних викликів. До основних перешкод варто віднести недостатній рівень нормативного закріплення функцій CDTO, відсутність системи мотивації, що стимулює професійний розвиток та утримання кваліфікованих фахівців, а також дефіцит компетентностей на місцях. Особливо критичною ця проблема є для територіальних громад, де відсутність фахівців із відповідним рівнем навичок ускладнює виконання стратегічних завдань цифрової трансформації місцевого рівня. Це зумовлює необхідність розробки єдиного державного стандарту професійних компетентностей CDTO та створення дієвих механізмів ресурсної підтримки цифрових офісів для подолання цифрового розриву між центром та регіонами.

Ситуація додатково загострюється відтоком спеціалістів у приватний сектор, а також обмеженими бюджетними можливостями для залучення висококваліфікованих кадрів. Крім того, органи влади часто демонструють інституційну інертність, що проявляється у неспроможності оперативно адаптувати управлінську модель до викликів цифровізації. Це створює додаткові бар'єри для реалізації комплексної та ефективної цифрової трансформації.

*На технологічному рівні* ризики пов'язані насамперед із питаннями кібербезпеки та захисту персональних даних. В умовах зростання кількості кібератак на інституції публічного сектору в Україні та за її межами, питання розбудови стійких кіберзахисних контурів набуває пріоритетного значення. До прикладу, у Великій Британії аудит кіберзахисту державних органів у 2025 році виявив, що 58 ключових систем є вразливими до атак через застарілі або фрагментовані ІТ-платформи [213].

Для України ці загрози актуалізуються через повномасштабне російське вторгнення і постійний тиск з боку зовнішніх кіберсуб'єктів. Ще одним істотним ризиком є технологічна нерівність між різними територіями: великі міста мають відносно розвинену інфраструктуру, в той час як малі громади - обмежений доступ до сучасних рішень, зокрема хмарних платформ і аналітики Big Data. Нарешті, залежність від закордонних постачальників хмарних сервісів, без національного еквіваленту або належного контрактного регулювання, створює ризики втрати доступу до критичних сервісів у разі політичної або комерційної турбулентності. Закон України «Про хмарні послуги» закладає підвалини для політики «цифрового суверенітету» однак потребує глибшого інституційного наповнення.

З огляду на викладене, доцільним є виокремлення ключових пріоритетних напрямів удосконалення механізмів цифрової взаємодії на кожному з трьох рівнів: національному, організаційному та технологічному (табл. 3.5).

На національному рівні пріоритетом є створення повноцінної нормативно-координаційної системи управління інтеперабельністю, яка передбачає делегування повноважень спеціалізованому органу з регламентації, моніторингу та впровадження міжвідомчої цифрової взаємодії. При цьому важливо забезпечити нормативну сумісність українського законодавства з європейськими підходами (зокрема, положеннями Interoperable Europe Act).

На організаційному рівні пріоритетними є розбудова внутрішнього цифрового аудиту, стандартизація функціонування цифрових офісів, а також функціональне наповнення вже існуючих посад CDTO. Впровадження CDTO в Україні розпочалося, однак ефективність цих посад обмежується відсутністю чіткого регламенту повноважень, механізмів координації та підтримки їхньої діяльності.

На технологічному рівні ключовими напрямками є запровадження національної хмарної інфраструктури, що зменшить залежність від зовнішніх провайдерів, розвиток етичного та прозорого використання штучного інтелекту,

а також впровадження Big Data-аналітики в діяльність органів публічної влади на основі даних із державних реєстрів, платформ і сервісів.

Таблиця 3.5

Пріоритетні напрями удосконалення механізмів цифрової взаємодії органів публічної влади: рівні, напрями, інструменти, цілі та ризики впровадження

<b>Рівень управління</b>	<b>Пріоритетні напрями</b>	<b>Ключові інструменти</b>	<b>Основні цілі</b>	<b>Потенційні ризики впровадження</b>
Національний	Інституційне оформлення інтероперабельності та координації цифрової взаємодії	Розширення повноважень Мінцифри; адаптація Interoperable Europe Act	Уніфікація цифрової взаємодії, правова визначеність, міжвідомча інтеграція	Опір з боку окремих ЦОВВ до централізованої координації інтероперабельності
Організаційний	Стандартизація та посилення ролі CDTO і цифрових офісів	Регламентация функцій CDTO; внутрішній цифровий аудит; підвищення цифрової компетентності	Підвищення керованості трансформаціями, кадрова стійкість, цифрове лідерство	Брак кваліфікованих кадрів, відсутність єдиного стандарту функцій, недостатня мотивація персоналу
Технологічний	Побудова суверенної цифрової інфраструктури та аналітичної спроможності	Розвиток хмарних сервісів; впровадження етичного ШІ; аналітика Big Data через дашборди	Масштабованість послуг, стійкість до ризиків, ефективність рішень, інклюзивність доступу до сервісів	Кіберзагрози, цифрова нерівність між громадами, технологічна нерівність, залежність від закордонних провайдерів

Джерело: складено автором

Таким чином, вдосконалення механізмів цифрової взаємодії органів публічної влади в Україні має ґрунтуватися на цілісному, багаторівневому підході. Стратегічний фокус повинен зміщуватися від локальних цифрових ініціатив до координаційної та аналітичної інтеграції, що базується на міжнародних практиках і глибокому розумінні внутрішньої управлінської логіки. Національна політика має задавати нормативний та інституційний вектор, організаційний рівень забезпечувати керованість та відповідальність трансформацій, а технологічний – слугувати фундаментом для інноваційної реалізації політик.

Аналіз пріоритетних напрямів удосконалення цифрової взаємодії органів публічної влади дозволив виявити системну взаємозалежність між нормативним, організаційним і технологічним рівнями. Рівень нормативного регулювання визначає рамки цифрової сумісності та відповідальності; організаційний рівень формує спроможність інституцій реалізовувати цифрову трансформацію; технологічний забезпечує інфраструктурну й аналітичну основу управлінських інновацій. Простежується також загальна тенденція до інтеграції технологій штучного інтелекту та управління на основі даних, проте без якісного кадрового супроводу й нормативної стабільності ці технології можуть залишитися декларативними. Відтак, ефективне впровадження цифрових рішень потребує поєднання технічної інноваційності, організаційної мобільності та нормативної передбачуваності.

Окремо варто окреслити роль органів місцевого самоврядування (ОМС) у системі міжвідомчої цифрової взаємодії, оскільки саме вони виступають ключовими «фронтowymi» користувачами електронних сервісів у відносинах з громадянами. Удосконалення цифрових механізмів на локальному рівні потребує диференційованого підходу, який враховує як обмеження інституційної та технічної спроможності громад, так і зростаючі очікування щодо швидкості, зручності й прозорості публічних послуг.

Насамперед, важливо забезпечити стійку інтеграцію ОМС у національні цифрові платформи, зокрема систему електронної взаємодії «Трембіта». Станом

на перший квартал 2025 року до цієї платформи було підключено 245 органів державної влади та місцевого самоврядування, з яких 40 - це органи місцевої влади. Вони забезпечують електронний обмін даними з центральними органами виконавчої влади в рамках реалізації 453 інтеграційних рішень [214]. «Трембіта» забезпечує безпечну, стандартизовану та масштабовану передачу інформації без дублювання або ручної обробки. Однак для ефективного функціонування цієї системи на місцях важливо не лише технічно підключити ОМС, а й забезпечити стабільну роботу модулів, навчання персоналу та регулярне оновлення локальної ІТ-інфраструктури. Рекомендовано запровадити регулярний аудит цифрових каналів громад, оновити технічну інфраструктуру та посилити навчальні програми для працівників ЦНАПів.

Другим напрямом є впровадження інструментів електронної демократії (e-democracy), які сприяють посиленню прозорості та громадянської участі. Як вказує Рада Європи, електронні петиції, онлайн-опитування, громадські слухання через цифрові платформи значно підвищують довіру громадян до влади [215].

У цьому контексті доцільним є запровадження інтегрованих рішень на кшталт платформи «E-DEM», яка вже використовується в низці громад. Поєднання таких платформ з інформаційними потоками «Трембіта» дасть змогу ОМС не лише фіксувати волевиявлення громадян, а й інтегрувати результати у внутрішні управлінські процеси.

Важливо також наголосити на значенні відкритих даних у діяльності ОМС. Постанова Кабінету Міністрів України № 835 від 21 жовтня 2015 року зобов'язує органи місцевого самоврядування публікувати набори даних у форматі open data, що відкриває нові можливості для аналітики, планування й підзвітності [216].

Водночас аналітична спроможність на місцях залишається низькою: громади часто не мають ані спеціалістів із data-аналітики, ані відповідного програмного забезпечення. Доцільним є створення локальних реєстрів даних, інтегрованих із Єдиною системою моніторингу розвитку регіонів (UGIS), яка функціонує згідно з постановою КМУ №522 від 18.05.2023 року [217].

Це дозволить поєднати локальні цифрові практики з загальнонаціональним плануванням та моніторингом.

Як зазначалось вище, окрему увагу варто приділити кадровому забезпеченню цифрової трансформації на місцевому рівні. Як показують дані проєкту EGOV4Ukraine, впровадження посад CDO у громадах відбувається нерівномірно, а більшість цифрових офісів функціонує без достатньої підтримки, чіткого регламенту та стабільного фінансування. Тому важливо не лише зберігати ці посади, а й забезпечити їх нормативне закріплення, системну підтримку з боку Мінцифри та розробити базові програми сертифікації для працівників ОМС, відповідальних за цифрові зміни. В іншому випадку зростає ризик залежності громад від зовнішніх консультантів або недержавних ІТ-провайдерів.

Таким чином, органи місцевого самоврядування як ключова ланка реалізації цифрових послуг потребують адресної підтримки у чотирьох пріоритетних напрямках: технічної інтеграції в національні цифрові платформи, впровадження елементів електронної демократії, посилення відкритості через публікацію даних і формування кадрового потенціалу цифрової трансформації. Вважаємо, що ці заходи спроможні забезпечити інституційну сталість цифрових сервісів на місцях та сприятимуть формуванню більш прозорого, відповідального та інклюзивного врядування на рівні територіальних громад.

Таким чином, ОМС можуть виступити каталізатором цифрових змін завдяки: системній взаємодії з державною інфраструктурою, активному діалогу з громадянами, аналітичному плануванню, кадровому розвитку. Це відповідає світовим стандартам e-Government, наближає Україну до європейських практик та сприяє розгортанню стійких цифрових сервісів на місцях.

Для ефективного впровадження запропонованих заходів удосконалення механізмів цифрової взаємодії органів публічної влади важливим є дотримання логіки етапного розвитку, що відповідає системно-інституціональному підходу до цифрової трансформації (*institutional capacity building model*). Це дозволяє гармонізувати технічні, нормативні та кадрові зрушення, забезпечуючи

поступовий перехід від фрагментованих ініціатив до цілісної цифрової екосистеми управління.

*Короткостроковий етап (0–12 місяців)* зосереджується на діагностиці поточного стану цифрової взаємодії. На цьому рівні основним є:

- аудит нормативної бази щодо інтеперабельності та її відповідності європейським стандартам;
- розробка проекту Положення про міжвідомчу координаційну структуру;
- проведення оцінки цифрової спроможності органів публічної влади, зокрема за моделлю CAF Digital або аналогічними матрицями;
- запуск пілотних цифрових офісів у ключових ЦОВВ;
- створення тестових полігонів для застосування Big Data у державних сервісах (наприклад, прогнозування навантаження на ЦНАПи).

*Середньостроковий етап (1–3 роки)* повинен охопити інституціалізацію процесів цифрового лідерства, стандартизацію цифрових процедур і закріплення протоколів міжвідомчої взаємодії. До завдань цього етапу входять:

- нормативне закріплення функцій посад CDTO (Chief Digital Transformation Officer) в усіх органах публічної влади;
- масштабування цифрових офісів із розробкою KPI ефективності (в т.ч. за методологією Balanced Scorecard);
- адаптація до стандартів Interoperable Europe через національні технічні специфікації;
- широке впровадження модулів «Трембіта» на місцевому рівні;
- створення національного репозитарію відкритих даних ОМС та інтеграція його з системами аналітики UGIS.

*Довгостроковий етап (понад 3 роки)* передбачає перехід від трансформаційних змін до сталого розвитку цифрового врядування. Його головні завдання:

- наділення Мінцифри відповідними повноваженнями з управління

інтероперабельністю (з мандатом, подібним до Interoperable Europe Board);

- розбудова єдиної національної хмарної платформи для зберігання та обробки державних даних;
- повна автоматизація рутинних управлінських функцій (напр., видача дозволів, верифікація документів) із використанням штучного інтелекту (AI);
- формування механізмів проактивного врядування, орієнтованого на життєві події громадян (life-event-based services);
- впровадження нормативних рамок етики алгоритмів та захисту даних на основі концепції «digital rights by design» - цифровий зазамовчуванням.

Цей поетапний підхід співвідноситься з підходами, запропонованими OECD (2019) у доповіді «Шлях до становлення публічного сектору, керованого даними» (The Path to Becoming a Data-Driven Public Sector), де підкреслюється важливість переходу від експериментальних цифрових рішень до стабільних аналітичних платформ, інтегрованих у прийняття управлінських рішень [218].

Результати цифрових змін мають проявлятися не лише у формальних показниках ефективності, але й у якісних змінах взаємодії між державою і громадянином, зростанні довіри, адаптивності системи управління до нових викликів. Відтак, очікувані результати реалізації запропонованих заходів повинні розглядатися в контексті як виходу (output), так і впливу (impact), відповідно до логіки оцінювання політик (policy evaluation logic).

*Зростання довіри громадян до цифрової держави.* Як свідчить європейська практика (наприклад, у Фінляндії та Естонії), прозорість процедур, доступність сервісів і дотримання принципів захисту персональних даних сприяють формуванню соціального капіталу, що підтримує державні інституції. Це особливо актуально для України в умовах зростаючого запиту на підзвітність органів влади та боротьбу з корупцією.

*Підвищення швидкості та якості публічних послуг.* Автоматизація процесів, включення елементів предиктивної аналітики та взаємодія з громадянами через мобільні застосунки («Дія», «єМалятко», локальні Smart City-платформи) зменшують транзакційні витрати для громадян і бізнесу.

*Раціоналізація державних ресурсів.* Перехід до хмарних сервісів дозволяє зменшити витрати на ІТ-інфраструктуру щонайменше на 25-30 %, а використання big data у прогнозуванні дозволяє знижувати надлишкові адміністративні витрати. Досвід Ізраїлю та Сінгапуру засвідчує, що ефективна інвестиція в digital-екосистему має повертатися впродовж 2-4 років через економію ресурсів.

*Підвищення аналітичної спроможності органів публічної влади.* Впровадження BI-дашбордів, предиктивної аналітики та індикаторів ефективності дозволяє не лише моніторити надання послуг, а й впливати на планування політик (policy shaping). Особливо актуальним це є у сфері охорони здоров'я, освіти, соціального захисту та надзвичайних ситуацій, де рішення мають ухвалюватися на основі оперативних даних.

*Цифрова рівність та інклюзія.* Завдяки уніфікації цифрових сервісів і створенню умов для доступу навіть у віддалених громадах, очікується зниження цифрової нерівності, особливо вразливої у сільських районах та серед маломобільних груп населення. Рівний доступ до цифрових прав і послуг сприятиме зміцненню соціальної згуртованості.

Вважаємо, що впровадження етапних заходів цифрової взаємодії дозволяє не лише модернізувати публічне управління, а й закладає основу для переходу до нової моделі управління data-driven, citizen-centric, resilient governance (управління на основі даних, з фокусом на потребах громадян і високою адаптивністю до зовнішніх і внутрішніх змін), що відповідає європейським стандартам та очікуванням українського суспільства.

У третьому розділі дослідження обґрунтовано шляхи удосконалення механізмів цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. Здійснено всебічний аналіз інтеперабельності інформаційних систем як системоутворювального чинника цифрової взаємодії, визначено її технічні, семантичні, організаційні, юридичні та політичні компоненти, з урахуванням міжнародного досвіду та національних

реалізаційних практик (платформа «Трембіта», законодавчі акти, цифрові сервіси).

Розкрито роль запровадження інтероперабельності інформаційних систем як чинника підвищення ефективності механізмів цифрової взаємодії. Розроблено типологію інформаційних потоків у публічному управлінні (вертикальні, горизонтальні, внутрішньоорганізаційні, транскордонні, громадські), що дозволяє глибше осмислити архітектуру цифрової взаємодії та виявити ключові точки для її оптимізації. Обґрунтовано доцільність застосування реінжинірингу управлінських процесів на основі моделювання AS-IS і TO-BE, із залученням сучасних інструментів – SMART-систем, штучного інтелекту, аналітики Big Data.

Проаналізовано європейські стандарти інтероперабельності, насамперед положення Європейської рамки інтероперабельності (EIF) та Регламенту Interoperable Europe Act. Доведено, що національна модель цифрової взаємодії має базуватись не лише на технічних рішеннях (зокрема, на платформі «Трембіта»), але й на чітко визначеній інституційній архітектурі координації цифрових процесів, з розмежуванням повноважень і відповідальності між ЦОВВ, органами місцевого самоврядування, профільними агенціями та спеціалізованими підрозділами.

Розроблено архітектурну модель механізмів цифрової взаємодії на засадах інтероперабельності інформаційних систем органів публічної влади, яка відображає багаторівневу структуру взаємозв'язків між технічними, організаційними, нормативними та кадровими компонентами, забезпечує уніфікований обмін даними між суб'єктами публічного управління та відповідає вимогам Європейської рамки інтероперабельності. Модель враховує типологію інформаційних потоків (вертикальних, горизонтальних, транскордонних), інтегрує підходи до реінжинірингу управлінських процесів (AS-IS / TO-BE), а також передбачає функції моніторингу, координації та підтримки цифрової взаємодії на національному, регіональному та місцевому рівнях.

Методологічно обґрунтовано та розроблено матрицю моніторингу

функціонування механізмів цифрової взаємодії органів публічної влади як вітчизняної оціночної методики. На основі порівняльного аналізу існуючих підходів (OECD Digital Government Index, CAF Digital, DESI) розроблено чотирикомпонентну структуру моніторингової матриці, що включає індикатори нормативної, організаційної, технологічної та кадрової спроможності. Запропоновано уніфіковану шкалу оцінювання з поясненням типів даних для розрахунку та методів агрегування результатів. Визначено, що ключовим завданням такого моніторингу має бути не лише виявлення слабких місць, а й формування цільових програм підвищення ефективності цифрової взаємодії. Підкреслено, що цифрова трансформація потребує системного аналізу не лише технічних, а й організаційно-управлінських та соціальних складових.

Сформульовано комплекс практичних рекомендацій щодо пріоритетних напрямів удосконалення механізмів цифрової взаємодії. Виділено три рівні реалізації: національний, організаційний та технологічний з відповідними пріоритетами, інструментами, цілями та потенційними ризиками. На національному рівні визначено необхідність наділення відповідними повноваженнями Мінцифри як координаційного органу з питань інтеперабельності, нормативної уніфікації цифрових процесів і закріплення технічних стандартів на рівні підзаконних актів. На організаційному рівні обґрунтовано доцільність розвитку внутрішнього цифрового аудиту, створення цифрових офісів і функціонального наповнення посад CDTO, які вже впроваджені, але діють без чіткої регламентації повноважень і ресурсної підтримки. На технологічному рівні акцент зроблено на розвитку національної хмарної інфраструктури, впровадженні Big Data-аналітики та створенні етичних рамок застосування штучного інтелекту.

Окрему увагу приділено органам місцевого самоврядування як ключовим користувачам міжвідомчої цифрової взаємодії. Показано, що без забезпечення рівного доступу ОМС до хмарних платформ, реєстрів, сервісів Trembita та інструментів аналітики, цифрова трансформація залишатиметься фрагментарною.

Обґрунтовано етапність реалізації рекомендацій: короткострокових (нормативний аудит, пілотні офіси, функціональне наповнення CDTO), довгострокових (наділення Мінцифри відповідними повноваженнями з управління інтероперабельністю, повна інтеграція хмарних платформ і аналітичних інструментів). Запропоновано перелік очікуваних ефектів: зростання довіри громадян до цифрової держави, підвищення якості та швидкості надання послуг, економія ресурсів, підвищення аналітичної спроможності управління та зменшення цифрової нерівності.

Основні результати дослідження, що викладені у третьому розділі, висвітлено у таких публікаціях автора: [151; 161; 162; 163; 176].

## ВИСНОВКИ

У дисертації викладено результати наукового дослідження щодо узагальнення науково-теоретичні основ та теоретико-методологічне обґрунтування механізмів цифрової взаємодії органів публічної влади та розробки практичних рекомендацій щодо удосконалення їх функціонування в умовах розвитку електронного урядування. Отримані узагальнюючі результати дозволяють сформулювати наступні висновки.

1. Аналіз стану наукових досліджень проблем цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування дав змогу окреслити багаторівневий характер цього явища, яке формується на перетині правових, організаційних, технологічних та соціально-комунікативних вимірів. У науковому полі простежується еволюція підходів: від первинного трактування цифровізації як інструменту автоматизації процесів до сучасного розуміння її як комплексного механізму трансформації публічного управління, заснованого на принципах людиноцентричності, прозорості, підзвітності та інклюзивності. Ця трансформація корелює з глобальними науковими тенденціями, що зосереджують увагу на формуванні концепцій *data-driven governance*, *citizen-centric governance* та *resilient governance*, які поступово інтегруються і в український науковий простір.

Засвідчено розмежування двох концептуальних ліній наукового пошуку: 1) техніко-технологічної, яка охоплює питання побудови цифрових систем, їх кіберзахисту і стандартизації та розвивається під впливом міжнародних ініціатив, зокрема Європейської рамки інтероперабельності, яка визначає загальноєвропейські стандарти сумісності; 2) соціо-гуманітарної, що фокусується на дослідженні змін управлінських практик, впровадженні людиноцентричних підходів, забезпеченні прозорості й публічної підзвітності, залученні громадян до процесів управління та зміцненні довіри до органів публічної влади. Вона активно взаємодіє з теоріями електронної демократії, інклюзивного врядування та соціального капіталу. Вказане підтверджує, що

подальші дослідження мають розвиватися у напрямі синергії цих вимірів.

Встановлено, що вітчизняні наукові розвідки характеризуються певною амбівалентністю: з одного боку, вони акумулюють глобальні тенденції цифрової трансформації, відображаючи прогресивні ідеї управління на основі даних, хмарних інфраструктур та використання ШІ, з іншого, фіксують бар'єри національного характеру, серед яких: політична фрагментація, нормативні прогалини, брак системності у формуванні політик та дефіцит кадрового забезпечення цифрових змін. Це дозволяє зробити висновок, що прагнення гармонізувати національну систему публічного управління із світовими стандартами супроводжується істотними труднощами внутрішньої адаптації, зумовленими політичною фрагментацією, нормативною незавершеністю та кадровими питаннями, що ускладнюють сталий розвиток електронного урядування.

Обґрунтовано, що дискурс щодо проблем цифрової взаємодії органів публічної влади постійно ускладнюється через стрімке зростання масштабів інноваційних розробок, їх архітектурну складність та міжсекторальне застосування, що актуалізує потребу в нових методологічних підходах до її дослідження.

2. Уточнення категоріально-понятійного апарату дослідження дало змогу систематизувати ключові дефініції, що окреслюють концептуальні рамки цифрової взаємодії органів публічної влади, а також виявити взаємозв'язки між ними. Обґрунтовано, що «електронне урядування» постає широкою управлінською парадигмою, яка інтегрує технологічні, правові та соціально-комунікативні процеси модернізації публічного управління. У межах цієї парадигми «цифрова взаємодія» визначається її функціональною складовою, що безпосередньо забезпечує обмін інформацією та даними між органами влади, громадянами та інституціями. «Інтероперабельність» виступає передумовою та базовою умовою цифрової взаємодії, оскільки саме вона гарантує узгодженість, сумісність і безперервність функціонування інформаційних систем у єдиному цифровому середовищі.

Установлено, що є чіткий взаємозв'язок між такими суміжними термінами: *електронне урядування* визначає загальну модель управління, *цифрова взаємодія* є її ключовим механізмом реалізації, а *інтероперабельність* – техніко-організаційною основою, що забезпечує функціональність і сталість цього механізму.

Особливу увагу приділено поняттю «механізми цифрової взаємодії органів публічної влади», яке запропоновано тлумачити як цілісний комплекс правових, організаційних, технологічних і комунікативних засобів, що у взаємодії формують основу для ефективного електронного урядування. Ця категорія має інтеграційний характер і дозволяє поєднати структурні (право, інституції, технічні рішення) та функціональні (процедури, практики, стандарти) компоненти, що в сукупності забезпечують результативність цифрових трансформацій.

Виявлено, що в наукових колах категорійно-понятійний апарат розвивається у кількох напрямках: *технологічному*, де цифрова взаємодія розглядається як інструмент забезпечення інтероперабельності, стандартизації даних, кіберзахисту та автоматизації адміністративних процедур; *комунікативному*, який наголошує на прозорості, підзвітності та участі громадян у цифровому просторі; *правовому*, що акцентує увагу на нормативній узгодженості, правових гарантіях захисту даних і регламентації цифрових процесів; *економічному*, де підкреслюється значення цифрової взаємодії як чинника оптимізації ресурсів, зниження трансакційних витрат і підвищення ефективності управлінських процесів.

3. З'ясовано, що механізми цифрової взаємодії та інтероперабельності інформаційних систем органів публічної влади в Україні перебувають на стадії інтенсивного становлення, характеризуючись поєднанням певних досягнень і водночас значних обмежень. Встановлено наявність нормативно-правових актів, які формують основу цифрової трансформації (концептуальні документи, Стратегія цифрового розвитку до 2030 р., рамки цифрових компетенцій тощо). Відзначено роль Міністерства цифрової трансформації як центрального

координатора цих процесів. Водночас підкреслено інституційну обмеженість поточного статусу Мінцифри: відсутність повноважень щодо затвердження обов'язкових технічних стандартів і механізмів нагляду за дотриманням міжвідомчих протоколів, що створює ризики фрагментації політики і «відособленого» розвитку цифрових ініціатив у ЦОВВ.

Зафіксовано головні технічні надбання і реалізовані рішення: запуск державної програми інформаційного обміну «Трембіта» (архітектура на основі X-Road), інтеграція з платформою «Дія», уніфікація форматів даних (JSON/XML) та створення реєстру метаданих, що свідчить про помітний прогрес у технічній інтероперабельності. Однак семантична інтероперабельність (узгодження термінології, метаданих, схем даних тощо) залишається ділянкою, що потребує пріоритетного наукового опрацювання.

Порівняння з провідними моделями зарубіжних держав показало, що успіх інтероперабельності гарантується не лише технічними платформами, а комплексом рішень: наявністю органу з мандатом на стандартизацію й контроль, постійними індикаторами моніторингу, навчальними програмами для державних кадрів та юридичними механізмами обов'язковості стандартів. У ЄС це прагнення втілено в підходах EIF та ініціативах, що передбачають мультиміріну інтероперабельність (технічну, семантичну, організаційну, юридичну, політичну), а також у створенні наднаціональних координаційних інституцій (Interoperable Europe Board). Провідні урядові служби (наприклад, GDS у Великій Британії) акцентують увагу на професійному цифровому розвитку кадрів як визначального чинника стійкої трансформації.

Підтверджено наявність кількох конкурентних переваг України: концентрації політичної волі і фінансової підтримки цифрових проектів у вигляді національних стратегій; реалізації техніко-технологічної інфраструктури («Трембіта», «Дія»); наявності нормативних ініціатив у сфері кібербезпеки та електронних послуг; широкої підтримки з боку міжнародних партнерів (EU4Digital та ін.). Ці елементи створюють платформу для подальшої консолідації інтероперабельності.

Окреслено основні вразливості та бар'єри: цифрова фрагментація, що насамперед зумовлена розпорошенням відповідальності між суб'єктами публічної влади; опір окремих ЦОВВ до централізованої координації; недостатність повноважень контролю та стандартизації у центрального координатора (Мінцифри); дефіцит семантичних стандартів і процедур; кадрова прогалина та нерівномірний розподіл технологічних можливостей між регіонами; ризики кібербезпеки та часткова залежність від зовнішніх хмарних провайдерів.

З'ясовано, що технологічні рішення (шини даних, хмарні сервіси, аналітичні дашборди) ефективні лише за умови підкріплення їх чіткою інституційною архітектурою: задокументованими повноваженнями, механізмами контролю виконання стандартів, процедурами сертифікації та постійним моніторингом. Показано, що перехід від «технологічної інтеграції» до «інтероперабельності за дизайном» (interoperability-by-design) вимагає одночасних змін у правовому полі, організаційній структурі та кадровій політиці.

4. Проаналізовано безпекові виклики та можливості цифрової взаємодії у системі органів публічної влади в Україні. Встановлено, що безпековий вимір цифрової взаємодії органів публічної влади в Україні має подвійний характер: загрозово-обмежувальний і водночас потенційно трансформаційний. Стрімке впровадження цифрових платформ і міжвідомчих сервісів підвищує вимоги до інформаційної та кібернетичної безпеки й одночасно породжує нові вразливості: недостатня законодавча деталізація у сфері кібербезпеки, відсутність єдиної, інституційно закріпленої стратегії кіберзахисту та розпорошення відповідальностей між різними суб'єктами публічної влади створюють організаційну основу для ризиків і уповільнюють оперативне реагування на інциденти. Крім того, обмеженість фінансових і технічних ресурсів стримує оновлення захисних засобів і підвищення кіберстійкості, а дефіцит кваліфікованих кадрів обмежує спроможності публічних структур проводити системні превентивні заходи й проводити ефективні інцидент-респонс операції.

Акцентовано, що технологічні інновації одночасно відкривають істотні

можливості підвищення безпеки та стійкості цифрових сервісів: використання IoT-рішень у поєднанні з автоматизованим моніторингом, впровадження блокчейн-ланцюгів для логування транзакцій, а також застосування модулів аналітичного моніторингу дають змогу створювати більш прозорі, відстежувані і криптографічно захищені ланцюги обробки даних. Підкреслено практичну цінність консолідованих міжвідомчих платформ («єдине вікно», державні програми інформаційного обміну) як інструменту централізованого контролю доступу й аудитів дій за умови, що такі платформи інструментально забезпечені механізмами прозорості використання даних для кінцевого користувача.

Виокремлено низку важливих напрямів для подолання виявлених загроз і реалізації потенціалу безпеки. Доцільним є запровадження гнучких, «чутливих» модулів ризик-менеджменту в побудову міжвідомчих платформ, що дозволить оцінювати ризики при впровадженні нових сервісів і сценаріїв обміну даними. Необхідне також інституціональне закріплення механізмів координації кібербезпеки на національному рівні. Підкреслено важливість інвестицій у людський капітал: цілеспрямовані програми навчання державних фахівців, підвищення кібергігієни серед працівників і громадян, а також стимулювання кооперації з приватним сектором і міжнародними партнерами для обміну знаннями й технологіями.

Акцентовано на необхідності підвищення прозорості платформ як елементу довіри: впровадження інструментів інформування користувачів про те, хто і з якою метою використовує їхні дані, а також доступних для громадськості звітів про інциденти створює передумови для зростання суспільної довіри і зниження ризику неконтрольованого використання персональних даних. Водночас необхідно формалізувати підходи до моніторингу й аудиту, що дозволить переходити від декларативних заходів до регулярного управлінського аналізу стану кіберзахисту.

5. Обґрунтовано практико-орієнтовані пропозиції щодо запровадження інтеперабельності інформаційних систем органів публічної влади як чинника удосконалення механізмів цифрової взаємодії. Доведено, що запровадження

інтероперабельності інформаційних систем є визначальним чинником удосконалення механізмів цифрової взаємодії органів публічної влади, оскільки саме вона забезпечує перехід від фрагментарних цифрових ініціатив до цілісної політики електронного урядування. Наголошено, що інтероперабельність варто розглядати не лише як технічну здатність систем до обміну даними, а як багатовимірну концепцію, що інтегрує організаційні, правові, інформаційні, технологічні та кадрово-ресурсні компоненти. Такий підхід відповідає провідним науковим традиціям європейських досліджень (European Interoperability Framework, 2017; Interoperable Europe Act, 2022), які акцентують на системності, людиноцентричності та прозорості публічних цифрових процесів.

Розроблено архітектурну модель механізмів цифрової взаємодії, що ґрунтується на принципах інтероперабельності інформаційних систем і має комплексний характер. Її цільово-функціональний блок (організаційна архітектура) визначає управлінські функції органів влади, структурує типові адміністративні процеси (надання послуг, реєстраційні процедури, видачу дозволів) і закріплює стратегічні пріоритети цифрової трансформації, серед яких прозорість, підзвітність і орієнтація на громадянина. Інформаційно-комунікативний блок (інформаційна архітектура) встановлює правила стандартизації, обігу та повторного використання даних, інтегруючи національні інформаційні ресурси через платформи на зразок «Трембіта» та портали відкритих даних. Сервісно-інтеграційний блок (прикладна архітектура) забезпечує практичну реалізацію управлінських функцій за допомогою цифрових сервісів, реєстрових шлюзів, систем електронного документообігу та відкритих API, створюючи екосистему для швидкої та безперервної взаємодії органів влади з громадянами й бізнесом. Інфраструктурно-технологічний блок (технічна архітектура) відповідає за сумісність і надійність інформаційних систем, включаючи хмарні та туманні інфраструктури, серверні платформи, засоби кіберзахисту та системи резервування даних. Кадрово-ресурсний блок (архітектура людського потенціалу) формує основу для розвитку цифрових

компетенцій державних службовців, створення системи підготовки кадрів, підвищення цифрової культури та стійкості до технологічних змін.

Запропонована модель інтегрує п'ять типів інтеоперабельності: технічну, семантичну, організаційну, юридичну та політичну. Це дозволяє формувати єдиний масштабований і безпечний інформаційний простір, у якому цифрова взаємодія органів публічної влади відбувається у стандартизованих, передбачуваних і захищених формах. Така архітектура є не лише теоретичною конструкцією, а й практичною дорожньою картою для створення цифрової держави, що базується на принципах *data-driven governance*, людиноцентричності та стійкості.

Розроблена архітектурна модель формує системний фундамент для сталого розвитку електронного урядування в Україні, гармонізованого з європейськими стандартами. Її впровадження дозволяє одночасно розв'язати проблеми фрагментації цифрових систем, посилити інституційну спроможність публічної влади, підвищити довіру громадян і закласти підвалини для подальшого інноваційного розвитку суспільства.

6. Розроблено комплексну оцінювальну методіку функціонування механізмів цифрової взаємодії органів публічної влади, яка інтегрує інструменти контролю, оцінки та організаційно-технічного забезпечення цифрових процесів і може слугувати операційною основою для формування *evidence-based policy* (політики, заснованій на доказах: науково перевірених даних, статистики, результатів досліджень, аналітики та емпіричних доказів) у сфері електронного урядування. Запропонована методіка подана у вигляді матриці моніторингу, що поєднує багатовимірні (технічні, семантичні, організаційні, правові та кадрові) групи індикаторів, різнотипні шкали вимірювання (кількісні, бінарні, якісні та агреговані індекси) і мультиджерельну систему збору даних (реєстри, технічні логи, нормативні акти, внутрішні звіти, опитування користувачів, фронт-офісна аналітика), що забезпечує репрезентативність і валідність отримуваних оцінок.

Методологічна структура матриці поєднує системний аналітичний підхід з емпіричною обґрунтованістю та адаптивністю до змін цифрового середовища: у

ній виокремлено базові компоненти (нормативний, організаційний, технологічний і кадрово-ресурсний), кожен із яких має набір індикаторів із чітко визначеним типом розрахунку (абсолютні величини, відносні показники, частотні характеристики, бальні шкали та агреговані індекси) і джерелом верифікації даних. Така багатокомпонентна модель забезпечує одночасне вимірювання зовнішньої ефективності цифрової взаємодії і внутрішньої спроможності органів публічної влади, що робить моніторинг придатним для оперативного менеджменту та стратегічного планування.

Методологія побудови матриці також закладає механізми зрівноваження об'єктивних технічних показників і суб'єктивних якісних оцінок: поряд із автоматичними метриками пропонується регулярне опитування користувачів сервісів і експертні оцінки для виявлення «неформальних» бар'єрів (процедурні, культурні, кадрові), що дозволяє матриці виявляти проблеми, які не відображаються в логах чи реєстрах. SWOT-аналіз, вбудований у процедуру первинної діагностики, дає змогу зіставити внутрішні спроможності та зовнішні ризики для планування кадрових, фінансових, інших заходів.

Головною інновацією в науковому та прикладному вимірі є поєднання трьох функціональних пластів у єдиному інструменті: 1) контрольний (аудит, сертифікація відповідності стандартам, перевірки виконання нормативних вимог); 2) оцінний (системне вимірювання продуктивності, якості послуг, доступності та задоволеності); 3) організаційно-технічний (автоматизований збір метрик через системні логи, API-виклики і дашборди, а також механізми зворотного зв'язку для корекції процесів).

7. Сформульовано комплекс рекомендацій щодо пріоритетних напрямів удосконалення механізмів цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування.

На національному рівні пріоритетом має стати інституційна консолідація управління інтероперабельністю: доведено доцільність наділення центрального координатора (Мінцифри або спеціалізованого агентства) чітким мандатом із регламентації технічних і семантичних стандартів, нагляду за їх дотриманням та

правом видавати обов'язкові настанови й сертифікації. Це дозволить подолати розпорошення повноважень і забезпечити уніфікацію підходів на підставі європейських практик (EIF, Interoperable Europe Act).

На організаційному рівні рекомендації концентруються на функціоналізації і масштабуванні внутрішніх інструментів управління цифровою трансформацією. Зокрема, обґрунтовано необхідність формалізації посад CDTO в усіх ЦОВВ і ОМС із чітко визначеними повноваженнями, KPI та ресурсною підтримкою; створення і масштабування цифрових офісів з уніфікованими процедурами внутрішнього цифрового аудиту; запровадження системи мотивування та утримання фахівців (кар'єрні треки, фінансові стимулювання, програми підвищення кваліфікації тощо). Ці заходи спрямовані на підвищення організаційної спроможності до впровадження інтеперабельних рішень та на забезпечення координації між вертикалями і горизонталями управління.

Технологічний блок рекомендацій передбачає поступове, проте цілеспрямоване нарощування інфраструктури й інструментів: розбудова національної хмарної платформи і стандартів «Cloud-First», масове впровадження на місцях модулів шини обміну («Трембіта») та уніфікованих API, створення національних репозиторіїв відкритих даних і єдиної семантичної карти (metadata catalogue). Одночасно необхідно розгорнути етичні та регуляторні рамки застосування ШІ, стандарти захисту даних і процедури кіберзахисту на рівні архітектури (secure-by-design), а також інструменти Big-Data-аналітики і дашбордів для оперативного прийняття рішень. Технологічні ініціативи мають супроводжуватися політикою, яка мінімізує ризики залежності від іноземних провайдерів та передбачає вимоги до локалізації й доступності критичних даних.

Реалізація запропонованих заходів дозволить сформувати ефективні механізми цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування, що відповідатимуть стратегічним цілям держави та інтеграційним орієнтирам України на шляху у європейський цифровий простір.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Радиш Я.Ф. Категорійно-понятійний апарат про державне управління (огляд літератури та уточнення окремих дефініцій). Вісн. УАДУ, 2001. № 1. С. 195-202.
2. Попов О. Analysis of terms and concepts «electronic government», «digital interaction of public authorities», «information systems». Sciences of Europe. Praha, 2022. № 107. P. 112-115.
3. Francisca Tejedo-Romero and ets. E-government mechanisms to enhance the participation of citizens and society: Exploratory analysis through the dimension of municipalities. Technology in Society. Volume 70, August 2022. URL: <https://www.sciencedirect.com/science/article/pii/S0160791X22001191> (дата звернення 09.01.2023)
4. UNDESA (2014) E-Government Survey 2014: E-Government for the future we want, United Nations, New York.
5. OECD (2022). Glossary of statistical terms. URL: <https://stats.oecd.org/glossary/detail.asp?ID=4752> (дата звернення 09.01.2023)
6. Organization of American States (2022). About e-Government. URL: <http://portal.oas.org/portal/sector/sap/departamentoparalagesti%C3%B3np%C3%BAblicaefectiva/npa/sobreprogramadeegobierno/tabid/811/default.aspx?language=en-us> (дата звернення 09.01.2023)
7. IGI Global (2022). What is Electronic Government (e-Government). URL: <https://www.igi-global.com/dictionary/investigating-enterprise-application-integration-adoption/9385> (дата звернення 20.02.2023)
8. The digital era for all. Axel van Trotsenburg. February 29, 2024. URL: <https://blogs.worldbank.org/en/voices/digital-era-all> (дата звернення 09.02.2023)
9. Про адміністративні послуги : Закон України URL: <https://zakon.rada.gov.ua/laws/show/5203-17#Text> (дата звернення 09.01.2023)
10. Урядовий портал. URL: <https://www.kmu.gov.ua/usi-pitannya-po-e-poslugam/sho-take-elektronna-posluga> (дата звернення 19.03.2023)

11. Про заходи щодо впровадження Концепції адміністративної реформи в Україні : Указ Президента України від 22 липня 1998 № 810/98. URL: <https://zakon.rada.gov.ua/laws/show/810/98#Text> (дата звернення 09.04.2023)
12. Louise Whittaker. Information Systems Evaluation: a post-dualist interpretation. URL: <https://repository.up.ac.za/bitstream/handle/2263/25520/00body.pdf?sequence=1&isAllowed=y> (дата звернення 15.04.2023)
13. Yuchong Li. A comprehensive review study of cyber-attacks and cyber security. Emerging trends and recent developments, 2021. URL: <https://www.sciencedirect.com/science/article/pii/S2352484721007289> (дата звернення 12.05.2023)
14. Lei Zhang, Yonggen Gu. Information Systems and Computing Technology. CRC Press; 1st edition (August, 2013) 180 p.
15. Matthew Martin. Types of Information System : MIS, TPS, DSS, Pyramid Diagram. URL: <https://www.guru99.com/mis-types-information-system.html> (дата звернення 21.02.2024)
16. Britannica (2022). Information system. URL: <https://www.britannica.com/topic/information-system>
17. Emeritus (2022). URL: What is Information System? Definition, Examples. & Facts. URL: <https://emeritus.org/in/learn/information-system/> (дата звернення 09.01.2023)
18. Master's in Data Science (2022). What is Information System? URL: <https://www.mastersindatascience.org/learning/what-is-an-information-system/> (дата звернення 14.06.2023)
19. The University of Alabama at Birmingham (2022). What is Information System? URL: <https://businessdegrees.uab.edu/blog/what-is-information-systems/> (дата звернення 19.01.2023)
20. Information Technology Laboratory (2022). Glossary. URL: [https://csrc.nist.gov/glossary/term/information\\_system](https://csrc.nist.gov/glossary/term/information_system) (дата звернення 22.02.2024)
21. Technopedia (2020). Information system. URL:

<https://www.techopedia.com/definition/24142/information-system-is> (дата звернення 09.05.2023)

22. Policy Highlights. The Digital Transformation of Small and medium-sized enterprises. URL: <https://www.oecd.org/industry/smes/PH-SME-Digitalisation-final.pdf> (дата звернення 11.04.2024)

23. Stephen O'Connor. What Is Interoperability, and Why Is it Important? URL: <https://www.adsc.com/blog/what-is-interoperability-and-why-is-it-important> (дата звернення 06.02.2024)

24. Ramya Mohanakrishnan. What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices. URL: <https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/> (дата звернення 05.04.2023)

25. Баранов О.А. Економіка результату, інтернет речей та право. Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали науково-практичної конференції, 10 грудня 2020 р., м. Київ / упоряд.: О.А. Баранов, В.М. Фурашев, С.О. Дорогих. Київ : Фенікс, 2020. 272 с.

26. Michael E. Porter, Victor E. Millar. How Information Gives You Competitive Advantage. Harvard Business Review. URL: [https://hbr.org/search?term=michael%20e.%20porter&search\\_type=search-all](https://hbr.org/search?term=michael%20e.%20porter&search_type=search-all) (дата звернення 09.01.2023)

27. Олешко Т. І., Касьянова Н. В., Смерічевський С. Ф. та ін. Цифрова економіка : підручник. Том I. К. : НАУ, 2022. 200 с.

28. Deanira Laze. Digitalization as a tool to reduce corruption in the Public Administration. URL: [https://www.ie-ei.eu/Ressources/FCK/image/Theses/2021/GEGPA\\_Thesis\\_Laze.pdf](https://www.ie-ei.eu/Ressources/FCK/image/Theses/2021/GEGPA_Thesis_Laze.pdf) (дата звернення 09.01.2024)

29. Education Innovation and Research. The power of digital technologies and skills. OECD 2016. URL: <https://www.oecd.org/education/ceri/GEIS2016-Background-document.pdf> (дата звернення 16.07.2024)

30. Interoperability: Webster's Timeline History, 1893 – 2007. Icon Group International, 2009. P. 138
31. Interoperability. Oxford English Dictionary. URL: <https://www.oxfordlearnersdictionaries.com/definition/english/interoperability> (дата звернення 09.01.2023)
32. Paul Miller. Interoperability: What Is It and Why Should I Want It? URL: <http://www.ariadne.ac.uk/issue/24/interoperability/> (дата звернення 19.01.2023)
33. IEEE. Advancing Technology for Humanity. Digital Library. URL: <https://ieeexplore.ieee.org/Xplore/home.jsp> (дата звернення 02.01.2024)
34. Integrate. Merriam-Webster online dictionary. URL: <https://www.merriam-webster.com/dictionary/integrate> (дата звернення 17.05.2023)
35. Jeremy Norman. Exploring the History of Information and Media through Timelines. URL: <https://www.historyofinformation.com/> (дата звернення 17.05.2023)
36. Herman Hollerith (1860 - 1929). Biography. University of St Andrews. URL: <https://mathshistory.st-andrews.ac.uk/Biographies/Hollerith/> (дата звернення 12.05.2023)
37. A short history of the Web. Accelerating science. URL: <https://home.cern/science/computing/birth-web/short-history-web> (дата звернення 14.05.2024)
38. The Modern History of Computing. Stanford Encyclopedia of Philosophy. URL: <https://plato.stanford.edu/entries/computing-history/> (дата звернення 19.10.2023)
39. Restructuring and Managing the Telecommunications Sector. A World Bank Symposium. URL: <https://documents1.worldbank.org/curated/zh/239461468740407441/pdf/multi-page.pdf> (дата звернення 19.10.2023)
40. Jim Finkle. IBM to roll out new mainframes despite shrinking market. URL: <https://www.reuters.com/article/us-ibm-mainframe-idUSBRE87R03S20120828> (дата звернення 13.10.2023)

41. Heidi Adkisson. A Brief History of Enterprise Computing. URL: <https://hpadkisson.medium.com/a-brief-history-of-enterprise-computing-part-2-73fa8f2ab9e4> (дата звернення 07.10.2023)
42. World Wide Web Foundation. History of the Web - World Wide Web Foundation. URL: <https://webfoundation.org/history-of-the-web/> (дата звернення 09.10.2023)
43. Public Administration and Development Management, Section 10 - Department for Development Support and Management Services", Volume I, Proposed Programme Budget for the Biennium 1994-1995, General Assembly, Official Records, FortyEighth Session, Supplement No.6 (A/48/6/Rev.1), the United Nations, New York, 1994. URL: [https://www.un.org/sites/un2.un.org/files/2020/06/a48-parti\\_0\\_0.pdf](https://www.un.org/sites/un2.un.org/files/2020/06/a48-parti_0_0.pdf) (дата звернення 10.09.2023)
44. Jalal Rezaeenour. Developing a Knowledge Management Metric Model Based on Balanced Scorecard Methodology. URL: [https://www.academia.edu/6316024/Developing\\_a\\_Knowledge\\_Management\\_Metric\\_Model\\_Based\\_on\\_Balanced\\_Scorecard\\_Methodology\\_An\\_Exploratory\\_Study](https://www.academia.edu/6316024/Developing_a_Knowledge_Management_Metric_Model_Based_on_Balanced_Scorecard_Methodology_An_Exploratory_Study) (дата звернення 19.10.2023)
45. Попов О.П. Историчні засади розвитку інформаційних систем, цифрової сумісності у взаємодії органів публічної влади. Інвестиції: практика та досвід. 2023. № 16. С. 233-238. URL: <https://nayka.com.ua/index.php/investplan/article/view/1953/1974> (дата звернення 11.11.2023)
46. Patrick Dunleavy, Helen Margetts. New Public Management Is Dead - Long Live Digital-Era Governance. URL: [https://www.researchgate.net/publication/228301216\\_New\\_Public\\_Management\\_Is\\_Dead\\_-\\_Long\\_Live\\_Digital-Era\\_Governance](https://www.researchgate.net/publication/228301216_New_Public_Management_Is_Dead_-_Long_Live_Digital-Era_Governance) (дата звернення 09.09.2023)
47. Електронне голосування: перспективи впровадження в Україні. Національний інститут стратегічних досліджень. URL: <https://niss.gov.ua/sites/default/files/2021-02/tokar-1.pdf> (дата звернення 09.09.2023)

48. International Monetary Fund. 2022. World Economic Outlook: War Sets Back the Global Recovery. Washington, DC. URL: <https://www.imf.org/-/media/Files/Publications/WEO/2022/April/English/text.ashx> (дата звернення 09.11.2023)

49. World Summit on Information Society Concludes First Phase by Adopting Declaration of Principles and Plan of Action. URL: <https://press.un.org/en/2003/pi1550.doc.htm> (дата звернення 21.11.2023)

50. Magdalena Kostoska. An Overview of Cloud Interoperability. Federated Conference On Computer Science And Information Systems. URL: [https://www.researchgate.net/publication/308200167\\_An\\_Overview\\_of\\_Cloud\\_Interoperability](https://www.researchgate.net/publication/308200167_An_Overview_of_Cloud_Interoperability) (дата звернення 07.05.2023)

51. 17 ways technology could change the world by 2027. URL: <https://www.weforum.org/agenda/2022/05/17-ways-technology-could-change-the-world-by-2027/> (дата звернення 13.09.2023)

52. Europe's Digital Decade. URL: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade#:~:text=The%20Digital%20Decade%20targets%20are,actions%20in%20the%20annual%20%20report> (дата звернення 07.05.2023)

53. Daniel Hodapp. Interoperability in the era of digital innovation: An information systems research agenda. Journal of Information Technology. Volume 37, Issue 4. P. 407-427.

54. Open Connectivity Foundation: Unlocking the Massive Opportunity in the Internet of Things. URL: <https://openconnectivity.org/> (дата звернення 05.05.2023)

55. Farrell J., T. Simcoe. Choosing the Rules for Consensus Standardization. URL: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f004f8085fd240cb996526adc15bd557ed69118b> (дата звернення 05.05.2023)

56. David J. Teece. Profiting from Innovation in the Digital Economy: Standards, Complementary Assets, and Business Models in the Wireless World. URL: [https://escholarship.org/content/qt58h69717/qt58h69717\\_noSplash\\_259dfc0380dba7](https://escholarship.org/content/qt58h69717/qt58h69717_noSplash_259dfc0380dba7)

[d7ee3405c2f4830014.pdf](#) (дата звернення 05.05.2023)

57. Ciriello R. F. Digital Innovation. Business and Information Systems Engineering. 2018, № 6. URL: [https://www.researchgate.net/publication/328148808\\_Digital\\_Innovation](https://www.researchgate.net/publication/328148808_Digital_Innovation) (дата звернення 05.05.2023)

58. Ondrus J., Gannamaneni A., Lyytinen K. The impact of openness on the market potential of multi-sided platforms: a case study of mobile payment platforms. URL: <https://journals.sagepub.com/doi/pdf/10.1057/jit.2015.7> (дата звернення 14.10.2023)

59. Mark de Reuver, Carsten Sorensen, Rahul C. Basole. The digital platform: a research agenda. Journal of Information Technology, 2018. № 33. URL: <https://journals.sagepub.com/doi/pdf/10.1057/s41265-016-0033-3> (дата звернення 15.09.2023)

60. Liu CZ., Gal-Or E, Kemerer CF, et al. Compatibility and proprietary standards: the impact of conversion technologies in IT markets with network effects. Information Systems Research. 2011, № 22 P. 188-207.

61. Interoperability In Digital Financial Services. CGAP/World Bank, 2021. URL: [https://www.cgap.org/sites/default/files/publications/2021\\_01\\_Technical\\_Note\\_Interoperability\\_Digital\\_Financial\\_Services.pdf](https://www.cgap.org/sites/default/files/publications/2021_01_Technical_Note_Interoperability_Digital_Financial_Services.pdf) (дата звернення 11.09.2023)

62. Lyytinen K. Digital product innovation within four classes of innovation networks. Information Systems Journal, 2016. № 26(1). P. 47-75.

63. Yoo Y, Boland RJ. Organizing for innovation in the digitized world. Organization Science, 2012. № 23(5). P. 398-408.

64. Wareham J., Fox P., Giner J. Technology Ecosystem Governance. Esade Working Paper N° 225-2. URL: [https://web.archive.org/web/20190308074323id\\_/http://pdfs.semanticscholar.org/ef3d/c061ae69987a42aa5f291f3c887b121e7797.pdf](https://web.archive.org/web/20190308074323id_/http://pdfs.semanticscholar.org/ef3d/c061ae69987a42aa5f291f3c887b121e7797.pdf) (дата звернення 19.10.2023)

65. Allen D., Karanasios S., Norman A. Information sharing and interoperability: the case of major incident management. European Journal of

Information Systems. 2017, № 23(4). P. 418-432

66. K. Karhu, R. Gustafsson, B. Eaton etc. Four Tactics for Implementing a Balanced Digital Platform Strategy. MIS quarterly executive. 2020, Vol.19 (2), pp.105-120.

67. E-Commerce and Digital Economy Program: Results of 2022. Moving Beyond Current Crises: Improving Digital Readiness in Developing Countries. URL: <https://unctad.org/publication/e-commerce-and-digital-economy-programme-year-review-2022> (дата звернення 24.09.2023)

68. Ingmar Lippert. Digitalisation as promissory infrastructure for sustainability. URL: <https://pure.itu.dk/en/publications/digitalisation-as-promissory-infrastructure-for-sustainability> (дата звернення 24.09.2023)

69. FixMyStreet: local community engagement in the UK. <https://www.centreforpublicimpact.org/case-study/public-engagement-in-uk>

70. SeeClickFix 311 CRM от CivicPlus. URL: <https://seeclickfix.com/> (дата звернення 25.09.2023)

71. National Government Services Portal. Government Service. URL: [https://services.india.gov.in/service/state\\_services?sd\\_id=448&ln=en](https://services.india.gov.in/service/state_services?sd_id=448&ln=en) (дата звернення 23.09.2023)

72. Lee Rainie, Barry Wellman. Networked: The New Social Operating System. URL: <https://direct.mit.edu/books/book/2187/NetworkedThe-New-Social-Operating-System> (дата звернення 24.09.2023)

73. Скорик О. О., Рябоконт Н. П. Цифрова трансформація моделі публічного управління: зарубіжний досвід та вітчизняні реалії. *Державне управління: удосконалення та розвиток*. 2020. № 7. URL: <http://www.dy.nayka.com.ua/?op=1&z=1704> (дата звернення 04.10.2022)

74. К.І. Сімаков, В.Г. Валіна, В.П. Лауніконіс, М.Ю. Будовій. Особливості державного управління в умовах цифрової трансформації України. *Економічний вісник Донбасу*. 2021, № 1(63), С. 179-185.

75. **Разумей Г.Ю.** Разумей М.М. Діджиталізація публічного управління як складник цифрової трансформації України. *Публічне управління та митне*

*адміністрування*. 2020, № 2 (25) С. 139-145.

76. Мохова Ю.Л. Державні механізми розвитку електронного урядування в умовах цифрових трансформацій України: автореф. доктора наук з державного управління / Мохова Юлія Леонідівна. Миколаїв, 2021. 42 с.

77. Чернецький С.С. Інформаційно-комунікаційне забезпечення сталого демократичного врядування в Україні/ Чернецький Сергій Сергійович. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування. - Маріупольський державний університет, м. Київ, 2023. URL: [http://mdu.in.ua/Nauch/spetsrada/DOCTOR/2023/Dis\\_Cherneckij.pdf](http://mdu.in.ua/Nauch/spetsrada/DOCTOR/2023/Dis_Cherneckij.pdf) (дата звернення 04.10.2022)

78. Романчук О.З. Електронне урядування: конституційно-правове дослідження: автореф. канд. юр. н. / Романчук Ольга Захарівна. Ужгород, 2020. 22 с.

79. Попов О.П. Дискурсне поле цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. Державне управління: удосконалення та розвиток. 2023, № 11. URL: <https://www.nayka.com.ua/index.php/dy/article/view/2444> (дата звернення 04.11.2024)

80. Про захист інформації в інформаційно-комунікаційних системах: закон України № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення 04.10.2024)

81. Про інформацію: закон України від 6 липня 1999 року № 2657-IV. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення 04.10.2024)

82. Про електронні документи та електронний документообіг: закон України від 22 травня 2003 року № 605-VII. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text> (дата звернення 04.10.2024)

83. Про захист персональних даних: закон України від 1 червня 2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата

звернення 04.10.2024)

84. Про доступ до публічної інформації: закон України від 13 січня 2011 року № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення 04.10.2024)

85. «Про Стратегію сталого розвитку «Україна-2020»: указ Президента України від 12 січня 2015 р. № 5/2015 URL: <https://zakon.rada.gov.ua/laws/show/5/2015#Text> (дата звернення 11.11.2024)

86. Про затвердження Порядку інтеграції інформаційних систем державних органів та органів місцевого самоврядування до Єдиного державного порталу адміністративних послуг : наказ Міністерства економічного розвитку і торгівлі України та Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України від 08.09.2016 № 1501/248. URL: <https://zakon.rada.gov.ua/laws/show/z1315-16#Text> (дата звернення 04.10.2024)

87. Про затвердження середньострокового плану пріоритетних дій Уряду до 2020 року та плану пріоритетних дій Уряду на 2017 рік: розпорядження Кабінету Міністрів України від 3 квітня 2017 р. № 275-р. URL: <https://zakon.rada.gov.ua/laws/show/275-2017-%D1%80#Text>

88. Про затвердження Порядку обміну інформацією між органами, що контролюють справляння надходжень бюджету, та органами місцевого самоврядування: постанова а Кабінету Міністрів Украї від 16 червня 2021 р. № 627. URL: <https://zakon.rada.gov.ua/laws/show/627-2021-%D0%BF#Text> (дата звернення 04.10.2024)

89. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження Кабінету Міністрів Україн від 20 вересня 2017 р. № 649-р. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text> (дата звернення 12.10.2024)

90. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів Україн від 17 січня 2018 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text> (дата

звернення 11.10.2024)

91. Про основні засади забезпечення кібербезпеки України: закон України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 07.10.2024)

92. Про затвердження плану заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019-2020 роки: розпорядження КМУ від 12 червня 2019 р. № 405-р. URL: <https://zakon.rada.gov.ua/laws/show/405-2019-%D1%80#Text> (дата звернення 04.10.2024)

93. Деякі питання цифрового розвитку: постанова Кабінету Міністрів України від 30 січня 2020 року № 56. URL: <https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text> (дата звернення 04.10.2024)

94. Про схвалення Стратегії розвитку сфери електронних комунікацій України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках: розпорядження Кабінету Міністрів України від 4 червня 2025 р. № 546-р. URL: <https://zakon.rada.gov.ua/laws/show/546-2025-%D1%80#Text> (дата звернення 11.11.2025)

95. Standards catalogue. <https://www.iso.org/standards-catalogue/browse-by-ics.html> (дата звернення 04.10.2022)

96. IEC 82045-1:2001. Document management. Part 1: Principles and methods. URL: <https://www.iso.org/ru/standard/34159.html> (дата звернення 14.10.2022)

97. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»: постанова Кабінету Міністрів України від 24.02.2003 р. № 208. URL: <https://zakon.rada.gov.ua/laws/show/208-2003-%D0%BF#Text> (дата звернення 04.10.2023)

98. Наказ Державного комітету зв'язку та інформатизації України «Про затвердження Переліку і Порядку надання інформаційних та інших послуг з використання електронної інформаційної системи «Електронний Уряд» № 149 від 15.08.2003 р. URL: <https://zakon.rada.gov.ua/laws/show/z1065-03#Text> (дата звернення 08.12.2023)

99. Куценко С. І. Перспективи розвитку нормативно-правового

забезпечення в контексті надання адміністративних послуг через електронні онлайн сервіси. Юридичний науковий електронний журнал. 2017. № 3. С. 89-92.

100. Інформаційно-аналітична система обліку звернень громадян «Звернення». URL: [https://id-software.org.ua/products\\_ua.html](https://id-software.org.ua/products_ua.html) (дата звернення 08.12.2022)

101. Державні послуги онлайн. URL: <https://diia.gov.ua/> (дата звернення 07.10.2024)

102. Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/> (дата звернення 16.12.2023)

103. Єдина інформаційна система соціальної сфери (ЄІССС). URL: <https://www.msp.gov.ua/e-servisy/yeiss> (дата звернення 06.11.2024)

104. Про порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: постанова Кабінету Міністрів №3/2002 від 04.01.2002. URL: <https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text> (дата звернення 04.10.2024)

105. Про електронну ідентифікацію та електронні довірчі послуги: закон України від 5 жовтня 2017 року № 2155-VIII URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення 18.10.2023)

106. Попов О.П. Цифрова взаємодія інформаційних систем органів публічної влади: аналіз світових практик. Актуальні питання у сучасній науці. 2025. № 1(31). С. 339-347. URL: <http://perspectives.pp.ua/index.php/sn/article/view/18792/18817> (дата звернення 14.12.2025)

107. Lee Rainie and Barry Wellman. Networked: The New Social Operating System. Cambridge. International Journal of Communication. MIT Press, 2013, № 7. 358 pp.

108. Попов О.П. Практика впровадження електронного урядування у Великобританії. Матеріали II міжнародної наукової конференції «Education and science of today: intersectoral issues and development of sciences» (м. Кембридж, Сполучене Королівство Великої Британії і Північної Ірландії, 18 серпня 2023) Р.

55-57. URL : <https://archive.logos-science.com/index.php/conference-proceedings/issue/view/14/14> (дата звернення 09.12.2024)

109. E-Government Survey 2022. The Future of Digital Government. URL: <https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf> (дата звернення 06.10.2024)

110. Choong-Sik Chung, Hanbyul Choi, Youngmin Cho. Analysis of Digital Governance Transition in South Korea: Focusing on the Leadership of the President for Government Innovation. URL: <https://www.sciencedirect.com/science/article/pii/S2199853122010113> (дата звернення 04.10.2024)

111. Denmark, Finland, the Republic of Korea, New Zealand and Iceland lead on e-government. URL: [https://www.wipo.int/global\\_innovation\\_index/en/gii-insights-blog/2023/e-government-development.html](https://www.wipo.int/global_innovation_index/en/gii-insights-blog/2023/e-government-development.html) (дата звернення 07.11.2024)

112. The new Danish Portal for Business - Virk.dk (VIRK). URL: <https://joinup.ec.europa.eu/collection/egovernment/document/new-danish-portal-business-virkdk-virk> (дата звернення 07.12.2023)

113. What is integrated Korea ON-line E-Procurement System (KONEPS)? URL: <https://pps.go.kr/eng/content.do?key=00777> (дата звернення 04.04.2024)

114. Smart Cities - South Korea. <https://www.statista.com/outlook/tmo/internet-of-things/smart-cities/south-korea> (дата звернення 17.05.2024)

115. The Benefits of Electronic Tax Administration in Developing Economies: A Korean Case Study and Discussion of Key Challenges. URL: <https://documents1.worldbank.org/curated/ar/246061561388336942/pdf/The-Benefits-of-Electronic-Tax-Administration-in-Developing-Economies-A-Korean-Case-Study-and-Discussion-of-Key-Challenges.pdf> (дата звернення 17.05.2024)

116. The Disruptive Fourth Industrial Revolution: Technology, Society and Beyond [1st ed.]. 2020. 285 P. URL: <https://dokumen.pub/the-disruptive-fourth-industrial-revolution-technology-society-and-beyond-1st-ed-9783030482299-9783030482305.html> (дата звернення 17.05.2024)

117. e-Identity. URL: <https://e-estonia.com/solutions/estonian-e-identity/e-residency/> (дата звернення 17.05.2024)
118. Public Private Partnerships. URL: [https://assets.publishing.service.gov.uk/media/5a7c7835e5274a559005a152/07\\_PPP\\_28.11.13.pdf](https://assets.publishing.service.gov.uk/media/5a7c7835e5274a559005a152/07_PPP_28.11.13.pdf) (дата звернення 21.05.2024)
119. Introducing GeBIZ and Learn How To Use. URL: <https://www.gebiz.gov.sg/> (дата звернення 21.05.2024)
120. Christine Zhenwei QiangCheow Hoe Chan. How Singapore's national digital identity and government digital data sharing platform fosters inclusion and resilience. 2022. URL: <https://blogs.worldbank.org/en/digital-development/how-singapores-national-digital-identity-and-government-digital-data-sharing> (дата звернення 17.05.2024)
121. Organisation of justice – judicial systems. Exercise of judicial power. URL: [https://e-justice.europa.eu/16/EN/national\\_justice\\_systems?SLOVAKIA&member=1](https://e-justice.europa.eu/16/EN/national_justice_systems?SLOVAKIA&member=1) (дата звернення 17.05.2024)
122. To the Future': Saudi Arabia Spends Big to Become an A.I. Superpower. URL: <https://www.nytimes.com/2024/04/25/technology/saudi-arabia-ai.html> (дата звернення 11.03.2024)
123. Swedish Social Insurance Agency selects CGI for development and digitalization services. URL: <https://www.cgi.com/en/swedish-social-insurance-agency-selects-cgi-for-digitalization-services> (дата звернення 17.05.2024)
124. Australian Taxation Office, ATO. Compare your business now. URL: <https://www.ato.gov.au/businesses-and-organisations/income-deductions-and-concessions/small-business-benchmarks/compare-your-business-now> (дата звернення 17.05.2024)
125. Robert Wallace Vaagan. Oslo Metropolitan University A Critical Analysis of the Digitization of Healthcare Communication in the EU: A Comparison of Italy, Finland, Norway, and Spain. URL: <https://ijoc.org/index.php/ijoc/article/view/15399> (дата звернення 17.05.2024)
126. Shafaq Khan. Mohammed Shael. Blockchain for Governments: The Case

of the Dubai Government. URL: <https://www.mdpi.com/2071-1050/14/11/6576> (дата звернення 11.05.2023)

127. Nicklas Holmberg. Service Orienting the Swedish Vaccination Recommendation Activity with the Business Rules Centric Digital Service VacSam. URL: [https://www.researchgate.net/publication/221581377\\_Service\\_Orienting\\_the\\_Swedish\\_Vaccination\\_Recommendation\\_Activity\\_with\\_the\\_Business\\_Rules\\_Centric\\_Digital\\_Service\\_VacSam](https://www.researchgate.net/publication/221581377_Service_Orienting_the_Swedish_Vaccination_Recommendation_Activity_with_the_Business_Rules_Centric_Digital_Service_VacSam) (дата звернення 17.03.2023)

128. Economy Profile of Singapore. Doing Business 2020 Indicators. URL: <https://www.doingbusiness.org/content/dam/doingBusiness/country/s/singapore/SGP.pdf> (дата звернення 18.04.2024)

129. The GDS Academy is here. Blog Government Digital Service. URL: <https://gds.blog.gov.uk/2017/07/27/the-gds-academy-is-here/> (дата звернення 17.05.2024)

130. Oleksandr Popov. Global trends in implementing innovative technologies into e-governance practices. «Scientific achievements of contemporary society»: materials of the I International Scientific and Practical Conference (London, United Kingdom. August 15-17, 2024) P. 328-331. URL: <https://sci-conf.com.ua/wp-content/uploads/2024/08/SCIENTIFIC-ACHIEVEMENTS-OF-CONTEMPORARY-SOCIETY-15-17.08.24.pdf> (дата звернення 18.05.2025)

131. Cyber security: A month in retrospect (Australia) - April 2025. URL: <https://www.hsfkramer.com/notes/cybersecurity/2025-posts/cyber-security-a-month-in-retrospect-australia-april-2025> (дата звернення 17.06.2025)

132. Data of half the population of France stolen in its largest ever cyberattack. This is what we know. URL: <https://www.euronews.com/next/2024/02/08/data-of-33-million-people-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we> (дата звернення 11.06.2025)

133. DIGITALISATION IN EUROPE 2021-2022. Evidence from the EIB Investment Survey. URL: [https://www.eib.org/files/publications/digitalisation\\_in\\_europe\\_2021\\_2022\\_en.pdf](https://www.eib.org/files/publications/digitalisation_in_europe_2021_2022_en.pdf)

(дата звернення 17.05.2024)

134. Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації: Закон України від 4 червня 2020 року № 681-IX. URL: <https://zakon.rada.gov.ua/laws/show/681-20#Text> (дата звернення 17.05.2024)

135. Постанова КМУ Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки від 23 грудня 2020 року № 1295. URL: <https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text> (дата звернення 21.06.2025)

136. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: постанова Кабінету Міністрів України від 4 квітня 2023 року № 299. URL: <https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text> (дата звернення 17.05.2024)

137. NIS 2.0 Directive – Comprehensive guide on NIS 2. <https://safereach.com/en/blog/nis-2-directive/> (дата звернення 28.05.2025)

138. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj> (дата звернення 17.05.2024)

139. Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua> (дата звернення 22.06.2025)

140. Національний координаційний центр кібербезпеки. URL: <https://report@ncsc.gov.ua/> (дата звернення 26.05.2024)

141. Галузевий центр кібербезпеки сприятиме забезпеченню надійного захисту підприємств енергетичного сектору. URL: <https://www.kmu.gov.ua/news/galuzevij-centr-kiberbezpeki-spriyatime-zabezpechennyu-nadijnogo-zahistu-pidpriyemstv-energetichnogo-sektoru> (дата звернення 15.06.2024)

142. Попов О.П. Безпекові аспекти цифрової взаємодії у системі органів

публічної влади в Україні. Інвестиції: практика та досвід. 2024. № 16. С. 309-314. URL: <https://www.nayka.com.ua/index.php/investplan/article/view/4396/4431> (дата звернення 14.06.2025)

143. T. Abrahams, S. Ewuga. A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, Volume 5, Issue 1, January 2024. URL: [https://www.researchgate.net/publication/377346019\\_A\\_review\\_of\\_cybersecurity\\_strategies\\_in\\_modern\\_organizations\\_examining\\_the\\_evolution\\_and\\_effectiveness\\_of\\_cybersecurity\\_measures\\_for\\_data\\_protection](https://www.researchgate.net/publication/377346019_A_review_of_cybersecurity_strategies_in_modern_organizations_examining_the_evolution_and_effectiveness_of_cybersecurity_measures_for_data_protection) (дата звернення 11.11.2025)

144. World Economic Forum. Why we need global rules to crack down on cybercrime. Jan 2, 2023. URL: <https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/> (дата звернення 17.09.2025)

145. Програма підвищення кваліфікації керівних кадрів у галузі знань «Цивільна безпека», за темою: «Цивільний захист». Категорія осіб: наукові та науково-педагогічні (педагогічні) працівники навчальних закладів та науково-дослідних установ. URL: [https://nuczu.edu.ua/images/topmenu/inform-pro-diyalnicti/navchalna-diyalnicti/pk\\_npp.pdf](https://nuczu.edu.ua/images/topmenu/inform-pro-diyalnicti/navchalna-diyalnicti/pk_npp.pdf) (дата звернення 14.05.2025)

146. Підвищення кваліфікації з питань кібербезпеки. Вища школа публічного управління при НАДС. URL: <https://hs.gov.ua/pidvishhennya-kvalifikaciyi-z-pitan-kiberbezpeki/> (дата звернення 21.06.2024)

147. SoftServe. Основи кібербезпеки. URL: <https://career.softserveinc.com/uk-ua/technology/course/cybersecurity-fundamentals> (дата звернення 17.05.2024)

148. Україна офіційно приєдналася до Центру НАТО з питань співробітництва в галузі кіберзахисту. URL: <https://www.ukrinform.ua/rubric-technology/3710022-ukraina-oficijno-priednalasa-do-centru-kiberzahistu-nato.html> (дата звернення 17.05.2024)

149. European Commission. European Interoperability Framework – Implementation Strategy. 2017. URL: <https://eur-lex.europa.eu/legal->

<content/EN/TXT/?uri=CELEX%3A52017DC0134> (дата звернення 10.05.2025)

150. European Declaration on Digital Rights and Principles. URL: <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> (дата звернення 17.05.2024)

151. Oleksandr Popov. Implementation of digital interaction in public administration. "Science And Innovation of Modern World": materials of the I International Scientific and Practical Conference (London, United Kingdom. 28-30 September, 2022) P. 354-357. URL : <https://sci-conf.com.ua/wp-content/uploads/2022/09/SCIENCE-AND-INNOVATION-OF-MODERN-WORLD-28-30.09.22.pdf> (дата звернення 07.07.2023)

152. Trembita.gov.ua – звіт за 1-й квартал 2025 року. URL: <https://eu4digitalua.eu/uk/news/trembita-gov-ua-zvit-za-1-j-kvartal-2025-roku/> (дата звернення 17.09.2025)

153. ЄС для цифрової України. URL: <https://eu4digitalua.eu/uk/> (дата звернення 06.05.2024)

154. Портал відкритих даних. URL: <https://data.gov.ua/> (дата звернення 14.06.2024)

155. Про особливості надання публічних (електронних публічних) послуг : Закон України. URL: <https://zakon.rada.gov.ua/laws/show/1689-20#Text> (дата звернення 04.05.2025)

156. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках : розпорядження КМУ № 1351-р від 31.12.2024. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> (дата звернення 17.05.2025)

157. В Україні розпочала роботу Координаційна Рада з розвитку цифрової економіки. URL: <https://me.gov.ua/News/Detail?lang=uk-UA&id=454449bd-5d28-4759-aa21-e93cf8e7f5d5&title=VUk> (дата звернення 11.07.2022)

158. Про схвалення Стратегії здійснення цифрового розвитку, цифрових

трансформацій і цифровізації системи управління державними фінансами на період до 2030 року та затвердження плану заходів щодо її реалізації : розпорядження КМУ від 17 листопада 2021 р. № 1467-р. URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text> (дата звернення 11.06.2022)

159. Рамка цифрової компетентності для громадян України. Міністерство цифрової трансформації України. 2021. URL: [https://thedigital.gov.ua/storage/uploads/files/news\\_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf](https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf) (дата звернення 14.06.2023)

160. Про затвердження Державної стратегії регіонального розвитку на 2021-2027 роки : постанова КМУ від 5 серпня 2020 р. № 695. URL: <https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text> (дата звернення 06.02.2024)

161. Oleksandr Popov. Digital interaction of public authorities. “Science And Technology: Problems, Prospects And Innovations”: materials of the I International Scientific and Practical Conference (Osaka, Japan. 19-21 October, 2022) P. 338-341. URL : <https://sci-conf.com.ua/wp-content/uploads/2022/10/SCIENCE-AND-TECHNOLOGY-PROBLEMS-PROSPECTS-AND-INNOVATIONS-19-21.10.22.pdf> (дата звернення 06.02.2024)

162. Oleksandr Popov. International standards of digital interaction of public authorities of Ukraine in the context of the development of electronic governance. «Science and society: modern trends in a changing world»: materials of the IX International Scientific and Practical Conference (Vienna, Austria, August 5-7, 2024) P. 216-219. URL: <https://sci-conf.com.ua/wp-content/uploads/2024/08/SCIENCE-AND-SOCIETY.-MODERN-TRENDS-IN-A-CHANGING-WORLD-5-7.08.24.pdf> (дата звернення 06.04.2025)

163. Oleksandr Popov. E-democracy as a tool for optimizing the interaction between government and citizens in the conditions of electronic government.

«Scientific progress: innovations, achievements and prospects» : materials of the VII International Scientific and Practical Conference (Munich, Germany. 3-4 April 2023) P. 400-404. URL : <https://sci-conf.com.ua/wp-content/uploads/2023/04/SCIENTIFIC-PROGRESS-INNOVATIONS-ACHIEVEMENTS-AND-PROSPECTS-3-5.04.23.pdf> (дата звернення 06.04.2025)

164. EGOV4UKRAINE. Project 2016-2021. Making data run, not people. URL: [https://ega.ee/wp-content/uploads/2021/08/Brochure\\_EGOV4Ukraine\\_EN\\_F.pdf?\\_gl=1\\*t8i8re\\*\\_up\\*MQ.\\*\\_ga\\*OTYyODE2NDgyLjE3NTg5OTU5NDU.\\*\\_ga\\_9FXJ5SMCDK\\*czE3NTg5OTU5NDQkbzEkZzAkdDE3NTg5OTU5NDQkajYwJGwwJGgw](https://ega.ee/wp-content/uploads/2021/08/Brochure_EGOV4Ukraine_EN_F.pdf?_gl=1*t8i8re*_up*MQ.*_ga*OTYyODE2NDgyLjE3NTg5OTU5NDU.*_ga_9FXJ5SMCDK*czE3NTg5OTU5NDQkbzEkZzAkdDE3NTg5OTU5NDQkajYwJGwwJGgw) (дата звернення 06.04.2025)

165. eHealth Digital Service Infrastructure. URL: <https://digitalhealtheurope.eu/glossary/ehdsi/> (дата звернення 16.04.2025)

166. Мінцифри представила досягнення та плани України щодо цифровізації адміністративних послуг на зустрічі з Європейською Комісією. URL: <https://www.kmu.gov.ua/news/mintsyfry-predstavyla-dosiahnennia-ta-plany-ukrainy-shchodo-tsyfrovizatsii-administratyvnykh-posluh-na-zustrichi-z-ievropeiskoju-komisiieju> (дата звернення 08.05.2025)

167. Хромова Ю.О. Особливості впровадження реінжинірингу у систему публічного управління в Україні. Актуальні проблеми державного управління. 2021. Том 1 № 82. URL: <http://uran.oridu.odessa.ua/article/view/229165> (дата звернення 06.04.2025)

168. Francesco Ciampi, Monica Faraoni, Jacopo Ballerini, Francesco Meli. The co-evolutionary relationship between digitalization and organizational agility: Ongoing debates, theoretical developments and future research perspectives. Technological Forecasting and Social Change, Vol. 176, 2022. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0040162521008143?via%3Dihub> (дата звернення 06.04.2025)

169. GovTech Maturity Index, 2022 Update: Trends in Public Sector Digital Transformation. URL:

<https://openknowledge.worldbank.org/entities/publication/10b535a7-e9d4-51bd-96ed-6b917d5eb09e> (дата звернення 06.04.2025)

170. Governing with artificial intelligence: are governments ready? OECD artificial intelligence papers. 2024. URL: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence\\_f0e316f5/26324bc2-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence_f0e316f5/26324bc2-en.pdf) (дата звернення 06.08.2025)

171. Digital Public Administration factsheets – 2023. URL: <https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2023> (дата звернення 06.08.2025)

172. UN E-Government Survey 2024. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024> (дата звернення 06.08.2025)

173. Про схвалення Стратегії цифрової трансформації соціальної сфери розпорядження КМУ від 28 жовтня 2020 р. № 1353-р. URL: <https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text> (дата звернення 06.08.2025)

174. Стандарт TOGAF, версія 9.2. URL: <https://surl.li/odsxjd> (дата звернення 26.05.2024)

175. Government Enterprise. Architecture Reference. URL: <https://cdrdv2-public.intel.com/828452/GEAR%20Logical%20and%20Physical.pdf>

176. Oleksandr Popov. Digitalization of the activities of public authorities. “Priority directions of science development” : materials of the V International Scientific and Practical Conference (Hamburg, Germany. 6-8 February 2023) P. 278-280. URL : <https://eu-conf.com/wp-content/uploads/2023/02/Priority-directions-of-science-development.pdf> (дата звернення 06.04.2025)

177. Бондарчук Н.В., Дуброва Н.П. Цифровізація публічного управління: стан та перспективи розвитку. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. 2023. Том 34 (73) № 1. URL: [https://www.pubadm.vernadskyjournals.in.ua/journals/2023/1\\_2023/38.pdf](https://www.pubadm.vernadskyjournals.in.ua/journals/2023/1_2023/38.pdf) (дата

звернення 16.04.2025)

178. О.Л. Коваленко, В.О. Хрутьба. Діджиталізація процесів управління змінами в умовах цифрової трансформації публічної сфери. Цифрова економіка та економічна безпека. 2024. № 6 (15), с. 401-407. URL: <http://dees.iei.od.ua/index.php/journal/article/view/550> (дата звернення 06.04.2025)

179. Europe's Digital Decade: digital targets for 2030. URL: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en) (дата звернення 06.08.2025)

180. The E-Leaders Handbook on the Governance of Digital Government. OECD. 2021. URL: [https://www.oecd.org/en/publications/the-e-leaders-handbook-on-the-governance-of-digital-government\\_ac7f2531-en.html](https://www.oecd.org/en/publications/the-e-leaders-handbook-on-the-governance-of-digital-government_ac7f2531-en.html) (дата звернення 11.04.2025)

181. The OECD Digital Government Policy Framework. Six dimensions of a Digital Government 2020. URL: [https://www.oecd.org/en/publications/the-oecd-digital-government-policy-framework\\_f64fed2a-en.html](https://www.oecd.org/en/publications/the-oecd-digital-government-policy-framework_f64fed2a-en.html) (дата звернення 06.05.2025)

182. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. URL: <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng> (дата звернення 06.05.2022)

183. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/868/oj> (дата звернення 05.05.2022)

184. Interoperable Europe Act. 2024. URL: <https://interoperable-europe.ec.europa.eu/interoperable-europe/interoperable-europe-act> (дата звернення 06.08.2025)

185. OECD Digital Government Index (DGI): Methodology and 2019 Results. URL: <https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/oecd->

[digital-government-index-dgi\\_1d12209c/b00142a4-en.pdf](#) (дата звернення 06.04.2025)

186. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023. URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L\\_202302841](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302841) (дата звернення 06.07.2025)

187. Noella Edelman, Nathalie Haug, Ines Mergel. University of Konstanz Digital Transformation in the Public Sector. Elgar Encyclopedia of Services. 2023. URL: [https://www.researchgate.net/publication/368632698\\_Digital\\_Transformation\\_in\\_the\\_Public\\_Sector](https://www.researchgate.net/publication/368632698_Digital_Transformation_in_the_Public_Sector) (дата звернення 06.04.2025)

188. Miriam Lips. Digital transformation in the public sector. Collaborating for Digital Transformation. 2024. URL: [https://www.researchgate.net/publication/377605593\\_Digital\\_transformation\\_in\\_the\\_public\\_sector](https://www.researchgate.net/publication/377605593_Digital_transformation_in_the_public_sector) (дата звернення 06.09.2025)

189. WBG GovTech Maturity Index: The State of Public Sector Digital Transformation; Washington, DC. World Bank (2021). URL: <https://documents1.worldbank.org/curated/en/495831623303257484/pdf/GovTech-Maturity-Index-The-State-of-Public-Sector-Digital-Transformation.pdf> (дата звернення 05.08.2025)

190. 2023 OECD Digital Government Index Results and key findings. URL: [https://www.oecd.org/en/publications/2023-oecd-digital-government-index\\_1a89ed5e-en.html](https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html) (дата звернення 06.04.2025)

191. Digital Decade 2024: eGovernment Benchmark. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark> (дата звернення 11.06.2025)

192. Національний інститут стратегічних досліджень. Цифрова трансформація економіки України. Березень 2025 року. URL: <https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-berezen-2025-roku> (дата звернення 16.11.2025)

193. Міністерство цифрової трансформації України. Результати

цифрової трансформації в регіонах України за 2024 рік. URL: <https://thedigital.gov.ua/news/rezultati-tsifrovoi-transformatsii-v-regionakh-ukraini-za-2024-rik> (дата звернення 06.07.2025)

194. The State of Digital Workplace Maturity in 2024. Gartner Research. URL: <https://www.gartner.com/en/documents/5344363> (дата звернення 06.04.2025)

195. Sanjana Gadabay. Cybersecurity Assessments. International Journal of Recent Technology and Engineering. 2020. URL: [https://www.researchgate.net/publication/363565569\\_Cybersecurity\\_Assessments](https://www.researchgate.net/publication/363565569_Cybersecurity_Assessments) (дата звернення 11.08.2025)

196. Deloitte Digital Maturity Index 2025. URL: <https://www.deloitte.com/de/de/issues/growth-competition/digital-maturity-index.html> (дата звернення 11.08.2025)

197. Матриця реформ в Україні 2025. URL: <https://reformmatrix.mof.gov.ua/> (дата звернення 06.04.2025)

198. E-Government Development Index (EGDI). URL: [https://data360.worldbank.org/en/dataset/UN\\_EGDI](https://data360.worldbank.org/en/dataset/UN_EGDI) (дата звернення 07.04.2025)

199. Україна посіла 5-те місце за індексом онлайн-сервісів у глобальному рейтингу ООН. 2024. URL: <https://thedigital.gov.ua/news/ukraina-posila-5-te-mistse-za-indeksom-onlayn-servisiv-u-globalnomu-reytingu-oon> (дата звернення 06.06.2025)

200. Про публічні електронні реєстри : Закон України. URL: <https://zakon.rada.gov.ua/laws/show/1907-20#Text> (дата звернення 06.06.2025)

201. European Commission. Interoperable Europe. IOPEU Monitoring. URL: <https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/interoperability-initiatives-ukraine> (дата звернення 06.06.2025)

202. REPORT on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). 2023. Report - A9-0254/2023 European Parliament. URL: <https://www.europarl.europa.eu/doceo/document/A-9-2023->

[0254\\_EN.html](#) (дата звернення 01.03.2025)

203. How WestRock Harnessed GenAI to Enhance Internal Audit. DELOITTE. The Wall Street Journal | CIO Journal. URL: <https://deloitte.wsj.com/cio/how-westrock-harnessed-genai-to-enhance-internal-audit-f8184951> (дата звернення 01.03.2025)

204. Paolo Ciancarini, Raffaele Giancarlo, Gennaro Grimaudo. Digital Transformation in the Public Administrations: a Guided Tour For Computer Scientists. Computer Science. Software Engineering. 2023. URL: <https://arxiv.org/abs/2305.05551> (дата звернення 06.04.2025)

205. The Path to Becoming a Data-Driven Public Sector. 2019. OECD Digital Government Studies. URL: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/the-path-to-becoming-a-data-driven-public-sector\\_9ed7e867/059814a7-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/the-path-to-becoming-a-data-driven-public-sector_9ed7e867/059814a7-en.pdf) (дата звернення 06.04.2025)

206. High-level expert group on artificial intelligence. European Commission. 2019. URL: <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> (дата звернення 11.04.2025)

207. Про хмарні послуги : Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text> (дата звернення 07.07.2025)

208. Електронна демократія та електронне урядування. 2020. URL: <https://uareforms.org/en/reforms/e-democracy> (дата звернення 12.05.2025)

209. Електронна демократія і врядування. URL: <https://uareforms.org/reforms/e-democracy> (дата звернення 06.05.2025)

210. Питання Міністерства цифрової трансформації : постанова КМУ від 18 вересня 2019 року №856. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text> (дата звернення 14.04.2025)

211. REPORT on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). A9-0254/2023. URL: [https://www.europarl.europa.eu/doceo/document/A-9-2023-0254\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2023-0254_EN.html) (дата

звернення 06.01.2024)

212. CDTO та цифрові лідерки громади. URL: <https://hromada.gov.ua/database/cdto> (дата звернення 06.01.2025)

213. Threat of cyber-attacks on Whitehall ‘is severe and advancing quickly’, NAO says. 2025. URL: <https://www.theguardian.com/technology/2025/jan/29/cyber-attack-threat-uk-government-departments-whitehall-nao> (дата звернення 06.10.2025)

214. Trembita.gov.ua – звіт за 1-й квартал 2025 року. URL: <https://eu4digitalua.eu/uk/news/trembita-gov-ua-zvit-za-1-j-kvartal-2025-roku/> (дата звернення 06.11.2025)

215. Council of Europe – Highlights 2021 (2022). URL: <https://edoc.coe.int/en/annual-activity-report/11344-council-of-europe-highlights-2021.html> (дата звернення 05.06.2023)

216. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : постанова КМУ від 21 жовтня 2015 р. № 835. URL: <https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text> (дата звернення 11.04.2022)

217. Про затвердження Порядку функціонування єдиної геоінформаційної системи здійснення моніторингу та оцінювання розвитку регіонів і територіальних громад : постанова КМУ від 23 травня 2023 р. № 522. URL: <https://zakon.rada.gov.ua/laws/show/522-2023-%D0%BF#Text> (дата звернення 06.10.2025)

218. OECD Digital Government Studies: The Path to Becoming a Data-Driven Public Sector. URL: [https://www.researchgate.net/publication/339500259\\_OECD\\_Digital\\_Government\\_Studies\\_The\\_Path\\_to\\_Becoming\\_a\\_Data-Driven\\_Public\\_Sector](https://www.researchgate.net/publication/339500259_OECD_Digital_Government_Studies_The_Path_to_Becoming_a_Data-Driven_Public_Sector) (дата звернення 06.09.2025)

## ДОДАТКИ

## Додаток А

**Список публікацій здобувача за темою дисертації та відомості про  
апробацію результатів дисертації**

**Статті в наукових фахових виданнях України категорії Б:**

1. Попов О.П. Історичні засади розвитку інформаційних систем, цифрової сумісності у взаємодії органів публічної влади. *Інвестиції: практика та досвід*. 2023. № 16. С. 233-238.

DOI: <http://doi.org/10.32702/2306-6814.2023.16.233>

URL: <https://nayka.com.ua/index.php/investplan/article/view/1953/1974>

2. Попов О.П. Дискурсне поле цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. *Електронний журнал «Державне управління: удосконалення та розвиток»*. 2023, № 11.

DOI: <http://doi.org/10.32702/2307-2156.2023.11.25>

URL: <https://www.nayka.com.ua/index.php/dy/article/view/2444>

3. Попов О.П. Безпекові аспекти цифрової взаємодії у системі органів публічної влади в Україні. *Інвестиції: практика та досвід*. 2024. № 16. С. 309-314.

DOI: <http://doi.org/10.32702/2306-6814.2024.16.309>

URL: <https://www.nayka.com.ua/index.php/investplan/article/view/4396/4431>

4. Попов О.П. Цифрова взаємодія інформаційних систем органів публічної влади: аналіз світових практик. *Актуальні питання у сучасній науці*. 2025. № 1(31). С. 339-347.

DOI: [https://doi.org/10.52058/2786-6300-2025-1\(31\)-339-347](https://doi.org/10.52058/2786-6300-2025-1(31)-339-347)

URL: <http://perspectives.pp.ua/index.php/sn/article/view/18792/18817>

**Статті у періодичних наукових виданнях інших держав, які входять до  
Організації економічного співробітництва та розвитку та/або**

**Європейського Союзу, з наукового напрямку, за яким підготовлено  
дисертацію здобувача:**

5. Popov O. Analysis of terms and concepts «electronic government», «digital interaction of public authorities», «information systems». Sciences of Europe. Praha, 2022. № 107. P. 112-115.

DOI: <https://doi.org/10.5281/zenodo.7479780>

URL: <https://www.europe-science.com/wp-content/uploads/2022/12/Sciences-of-Europe-No-107-2022.pdf>

**Публікації, які засвідчують апробацію матеріалів дисертації:**

6. Oleksandr Popov. Implementation of digital interaction in public administration. “Science And Innovation Of Modern World”: materials of the I International Scientific and Practical Conference (London, United Kingdom. 28-30 September, 2022) P. 354-357.

7. URL: <https://sci-conf.com.ua/wp-content/uploads/2022/09/SCIENCE-AND-INNOVATION-OF-MODERN-WORLD-28-30.09.22.pdf>

8. Oleksandr Popov. Digital interaction of public authorities. “Science And Technology: Problems, Prospects And Innovations” : materials of the I International Scientific and Practical Conference (Osaka, Japan. 19-21 October, 2022) P. 338-341.

URL: <https://sci-conf.com.ua/wp-content/uploads/2022/10/SCIENCE-AND-TECHNOLOGY-PROBLEMS-PROSPECTS-AND-INNOVATIONS-19-21.10.22.pdf>

9. Oleksandr Popov. Digitalization of the activities of public authorities. “Priority directions of science development” : materials of the V International Scientific and Practical Conference (Hamburg, Germany. 6-8 February 2023) P. 278-280.

URL: <https://eu-conf.com/wp-content/uploads/2023/02/Priority-directions-of-science-development.pdf>

10. Oleksandr Popov. E-democracy as a tool for optimizing the interaction between government and citizens in the conditions of electronic government.

«Scientific progress: innovations, achievements and prospects» : materials of the VII International Scientific and Practical Conference (Munich, Germany. 3-4 April 2023) P. 400-404.

URL: <https://sci-conf.com.ua/wp-content/uploads/2023/04/SCIENTIFIC-PROGRESS-INNOVATIONS-ACHIEVEMENTS-AND-PROSPECTS-3-5.04.23.pdf>

11. Олександр Попов. Практика впровадження електронного урядування у Великобританії. Матеріали II міжнародної наукової конференції «Education and science of today: intersectoral issues and development of sciences» (м. Кембридж, Сполучене Королівство Великої Британії і Північної Ірландії, 18 серпня 2023) P. 55-57.

URL:<https://archive.logos-science.com/index.php/conference-proceedings/issue/view/14/14>

12. Oleksandr Popov. International standards of digital interaction of public authorities of Ukraine in the context of the development of electronic governance. «Science and society: modern trends in a changing world»: materials of the IX International Scientific and Practical Conference (Vienna, Austria, August 5-7, 2024) P. 216-219.

URL:<https://sci-conf.com.ua/wp-content/uploads/2024/08/SCIENCE-AND-SOCIETY.-MODERN-TRENDS-IN-A-CHANGING-WORLD-5-7.08.24.pdf>

13. Oleksandr Popov. Global trends in implementing innovative technologies into e-governance practices. «Scientific achievements of contemporary society»: materials of the I International Scientific and Practical Conference (London, United Kingdom. August 15-17, 2024) P. 328-331.

URL:<https://sci-conf.com.ua/wp-content/uploads/2024/08/SCIENTIFIC-ACHIEVEMENTS-OF-CONTEMPORARY-SOCIETY-15-17.08.24.pdf>

**Апробація результатів дослідження** здійснювалася у доповідях та повідомленнях на наукових конференціях: «Science And Innovation Of Modern World» (Лондон, Велика Британія, 28–30 вересня 2022 р.); «Science And

Technology: Problems, Prospects And Innovations» (Осака, Японія, 19-21 жовтня 2022 р.); «Priority Directions of Science Development» (Гамбург, Німеччина, 6-8 лютого 2023 р.); «Scientific Progress: Innovations, Achievements and Prospects» (Мюнхен, Німеччина, 3-4 квітня 2023 р.); «Education and Science of Today: Intersectoral Issues and Development of Sciences» (Кембридж, Велика Британія, 18 серпня 2023 р.); «Science and Society: Modern Trends in a Changing World» (Відень, Австрія, 5-7 серпня 2024 р.); «Scientific Achievements of Contemporary Society» (Лондон, Велика Британія, 15-17 серпня 2024 р.).

## Довідки про впровадження результатів дисертаційного дослідження та участь у науково-дослідних роботах



### УКРАЇНА ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

Майдан Незалежності, будинок 2, м. Хмельницький, 29005  
тел. 0382 76-59-98, 76-45-17

E-mail: oblrada@km-oblrada.gov.ua

Web: km-oblrada.gov.ua

Код ЄДРНОУ 00022651

18.12.2025 № 2080/01-11

На № \_\_\_\_\_ від \_\_\_\_\_

#### ДОВІДКА про впровадження результатів дисертаційного дослідження Попова Олександра Павловича

Результати дисертаційного дослідження аспіранта кафедри менеджменту та бізнес-адміністрування Прикарпатського національного університету імені Василя Стефаника Попова Олександра Павловича на тему: «Механізми цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування» на здобуття ступеня доктора філософії з галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування» були використані Хмельницькою обласною радою при підготовці Стратегії регіонального розвитку Хмельницької області на 2021-2027 роки (оновлена редакція, затверджена рішенням обласної ради №13-26/2025 від 18 червня 2025 року).

Зокрема, пропозиції щодо запровадження програм розвитку цифрового лідерства та підвищення кваліфікації публічних службовців були враховані при формуванні Завдань Стратегії щодо посилення інституційної стійкості та кадрової спроможності обласних та місцевих органів влади.

Крім того, пропозиції щодо запровадження механізмів проактивного врядування, орієнтованого на життєві події громадян, враховано при обґрунтуванні необхідності підвищення аналітичної спроможності обласної ради для прийняття управлінських рішень на основі оперативних цифрових даних.

Голова обласної ради



Віолета ЛАБАЗЮК



УКРАЇНА  
ХМЕЛЬНИЦЬКА ОБЛАСТЬ  
ГОРОДОЦЬКА МІСЬКА РАДА  
ВИКОНАВЧИЙ КОМПІТЕТ

вул.Грушевського,53, м.Городок, Хмельницька область, 32000, тел.(03851)3-18-33,  
e-mail: rada@gorodocka-gromada.gov.ua ,http://gorodocka.gromada.gov.ua,  
код ЄДРПОУ 38823893

10.10.2025 № 38  
на № \_\_\_\_\_ від \_\_\_\_\_ р.

**Д О В І Д К А**  
**про впровадження результатів**  
**дисертаційного дослідження Попова Олександра Павловича**

Результати дисертаційного дослідження аспіранта кафедри менеджменту та бізнес-адміністрування Прикарпатського національного університету імені Василя Стефаника Попова Олександра Павловича на тему «Механізми цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування» на здобуття ступеня доктора філософії з галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування» були використані Городоцькою міською територіальною громадою Хмельницького району Хмельницької області. Зокрема, практичні пропозиції щодо посилення цифрової компетентності посадових осіб місцевого самоврядування (зокрема тих, хто працює із соціально вразливими сім'ями) були враховані у плануванні тренінгів для підвищення їхніх цифрових навичок та вміння працювати з інтегрованими інформаційними системами для обміну даними, а також використані при розробці внутрішнього Регламенту роботи з державними реєстрами при наданні адміністративних послуг.

Керуюча справами (секретар)  
виконавчого комітету



Ольга БИСТРИЦЬКА



УКРАЇНА

ДМИТРІВСЬКА СЕЛИЩНА РАДА  
НІЖИНСЬКИЙ РАЙОНУ ЧЕРНІГІВСЬКОЇ ОБЛАСТІ

ВИКОНАВЧИЙ КОМПЕТ

вул.Незалежності,18, с-ще.ДМИТРІВКА, 16572, тел. 45246,45247

22.09.2025 № 03-17/180

Довідка

про впровадження результатів  
дисертаційного дослідження Попова Олександра Павловича

Результати дисертаційного дослідження аспіранта кафедри менеджменту та бізнес-адміністрування Прикарпатського національного університету імені Василя Стефаника Попова Олександра Павловича на тему "Механізми цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування" на здобуття ступеня доктора філософії з галузі знань 28 "Публічне управління та адміністрування" за спеціальністю 281 "Публічне управління та адміністрування" були використані Дмитрівською громадою Ніжинського району Чернігівської області при підготовці Плану заходів Дмитрівської селищної ради на 2025-2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року.

Зокрема, пропозиції щодо цифрової рівності та інклюзії були враховані при формуванні заходів щодо забезпечення доступності за адаптації електронних послуг громади (веб-сайту, електронних реєстрів) до міжнародних вимог стандартів безбар'єрності (WCAG 2.1-Настанови із забезпечення доступності веб-контенту, версія 2.1.), що дозволяє забезпечити рівний доступ до інформації і сервісів для всіх мешканців, включаючи маломобільні групи населення та осіб з порушеннями зору.

Селищний голова



Валентин БОЙКО

**Систематизація нормативно-правових актів, що визначають концептуальні засади формування механізмів цифрової взаємодії інформаційних систем органів публічної влади в Україні в умовах розвитку електронного урядування**

<b>Рік</b>	<b>Назва закону/підзаконного акту</b>	<b>Загальні положення</b>
1994	Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР [80]	Встановлює правові засади захисту інформації в електронних системах, визначає обов'язки суб'єктів у сфері забезпечення безпеки інформаційних ресурсів, підкреслює значення конфіденційності, цілісності та доступності даних.
1999	Закон України «Про інформацію» № 2657-IV [81]	Визначає основні принципи інформаційної політики, встановлює порядок доступу до інформації та взаємодії між органами влади, створюючи основу для формування відкритого та цифрового суспільства.
2003	Закон України «Про електронні документи та електронний документообіг» № 605-VII [82]	Запроваджує правові засади електронного документообігу, використання електронних підписів та печаток, підвищує ефективність роботи органів влади та забезпечує юридичну значущість електронних документів.
2010	Закон України «Про захист персональних даних» № 2297-VI [83]	Закріплює правові механізми збору, обробки, зберігання та знищення персональних даних громадян, встановлює відповідальність за порушення правил обробки персональних даних та забезпечує конфіденційність у цифровому середовищі.
2011	Закон України «Про доступ до публічної інформації» № 2939-VI [84]	Закріплює право громадян на доступ до інформації, що знаходиться у володінні органів влади та інших розпорядників публічної інформації, сприяє прозорості та підзвітності органів влади.
2015	Указ Президента України № 5/2015 «Про Стратегію сталого розвитку «Україна-2020»» [85]	Визначає розвиток електронного урядування одним із пріоритетів реформування публічного управління, закладає стратегічні орієнтири щодо цифровізації державних послуг, підвищення їхньої якості та доступності.
2016	Наказ МЕРТ та Мінрегіону № 1501/248	Встановлює порядок інтеграції інформаційних систем державних органів та органів місцевого

	86 «Про затвердження Порядку інтеграції інформаційних систем державних органів та органів місцевого самоврядування до Єдиного державного порталу адміністративних послуг» [86]	самоврядування до Єдиного державного порталу адміністративних послуг, централізує надання електронних послуг, автоматизує міжвідомчу взаємодію, підвищує доступність державних сервісів.
2017	Розпорядження КМУ № 275-р «Про затвердження середньострокового плану пріоритетних дій Уряду до 2020 року та плану пріоритетних дій Уряду на 2017 рік» [87]	Затверджує середньостроковий план пріоритетних дій Уряду до 2020 року та план на 2017 рік, визначає розвиток електронного урядування стратегічним пріоритетом модернізації публічного управління.
2017	Розпорядження КМУ № 649-р «Про схвалення Концепції розвитку електронного урядування в Україні» [89]	Визначає засади створення ефективної, прозорої та доступної системи публічного управління за допомогою ІКТ, забезпечує доступ громадян та бізнесу до державних послуг в електронному форматі, підвищує ефективність діяльності органів влади.
2018	Розпорядження КМУ № 67-р «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки» [90]	Визначає ключові напрями цифрової трансформації адміністративних процесів, підтримує реалізацію «Цифрової адженди України 2020», передбачає розвиток електронного документообігу, цифрової економіки, експорт цифрових технологій та підвищення цифрових компетенцій суспільства.
2017	Закон України «Про основні засади забезпечення кібербезпеки України» [91]	Встановлює правові та організаційні основи захисту життєво важливих інтересів громадян, суспільства та держави у кіберпросторі, визначає цілі та принципи державної політики в сфері кібербезпеки, повноваження органів та громадян.
2019	Розпорядження КМУ № 405-р «Про затвердження плану заходів щодо реалізації Концепції розвитку	Визначає пріоритетні напрями розвитку електронної демократії, розвиток цифрових каналів комунікації між органами влади та громадянами, запровадження електронного голосування, референдумів та плебісцитів,

	електронної демократії на 2019-2020 роки» [92]	інтеграцію електронних інструментів у різні сфери управління.
2020	Постанова КМУ № 56 «Деякі питання цифрового розвитку» [93]	Розроблено методичні рекомендації для реалізації принципів державної політики цифрового розвитку органами виконавчої влади, визначає взаємодію з органами влади, громадянами та бізнесом.
2021	Постанова КМУ № 627 «Про затвердження Порядку обміну інформацією між органами, що контролюють справляння надходжень бюджету, та органами місцевого самоврядування» [88]	Визначає порядок обміну інформацією між органами, що контролюють бюджетні надходження, та органами місцевого самоврядування, стандартизує та автоматизує міжвідомчий обмін даними, підвищує ефективність контролю та фінансової звітності.
2025	Розпорядження КМУ № 546-р «Про схвалення Стратегії розвитку сфери електронних комунікацій України на період до 2030 року» [94]	Забезпечує сталий розвиток електронних комунікацій, надання доступних послуг на всій території України, сприяння конкуренції та ефективним інвестиціям, науково-технічна та кадрова підтримка цифрової інфраструктури.