

Шевченко О. О.

Донбаська державна машинобудівна академія

Летенко В. В.

Донбаська державна машинобудівна академія

МЕХАНІЗМ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇНИ

У статті представлено обґрунтування питання вдосконалення алгоритму можливості змін системи електронного урядування в контексті забезпечення інформаційної безпеки країни; проаналізовано загальні аспекти е-урядування у форматі застосування цифрового публічного управління; розкрито основу електронного урядування як багатокомпонентної системи (враховуючи технологічний, нормативно-правовий, інституційний, соціальний та інформаційно-безпековий складові тощо), у комплексному підході (системність та застосування основ електронного урядування до угод цифрової трансформації); проаналізовано та наведено основні принципи прозорості, інтерактивності, доступності, ефективності, безпеки, інклюзивності е-урядування, що надає базу для подальшої еволюції цифрової взаємодії уряду і суспільства; опрацьовано функції електронного урядування, алгоритм взаємозв'язку між інформаційною безпекою і електронним урядуванням, за умов, що рівень застосування безпекових питань структуровано охоплює запити громад, функціональні вправи електронного урядування, моделі захисту інформації, а також структуру та вплив кіберзагроз на елементи захисту; проведено аналіз вітчизняної нормативно-законодавчої бази щодо створення інформаційної безпеки у сфері електронного урядування задля виявлення недоліків чинного законодавства та необхідності його пристосування до сучасних викликів; розкрито характер сучасних погроз безпеки інформації, визначено основні ризики, що проявляються перед електронним урядуванням в Україні, що дозволило глибше усвідомити проблематику питання в умовах війни; обґрунтовано стратегічні напрямки еволюції електронного урядування з в частині інформаційної безпеки; досліджено перспективну модель планування, за умов поетапного аналізу стратегічних вправ до вивчення; запропоновано покращення моделі проведення державної регіональної політики в сфері електронного урядування на рахунок просторових структурних змін цифрової інфраструктури, варіативного доступу до електронних послуг, регіональних ризиків на рівні територіальних громад та загальних загроз інформаційній безпеці.

Ключові слова: модернізація, місцеве самоврядування, публічне управління, е-урядування, інформація.

Постановка проблеми. Цифрові зрушення сучасності зумовлюють суттєві зміни в організації діяльності органів державної влади та органів місцевого самоврядування. На сьогодні одним із ключових інструментів такого перетворення виступає е-урядування, яке забезпечує доступність, прозорість та ефективність публічного управління з використанням цифрових технологій. Проте, одночасно з розвитком застосування цифрових сервісів зростає і рівень можливих інформаційних ризиків, що актуалізує питання дотримання інформаційної безпеки як ключової умови довіри до державних електронних платформ. На сьогодні в умовах війни, загроз кібербезпеці, активізації

бойових дій, потреба у побудові стійкої системи електронного урядування в державі, яка базується на належних стандартах захисту даних і цифрової довіри, є надзвичайно актуальною. При цьому, важливим є використання міжнародного досвіду провідних країн, які вже досягли певного прогресу щодо впровадження цифрового уряду та побудові комплексу інформаційної безпеки.

Потреба в проведенні оцінки взаємозв'язку між електронним урядуванням і інформаційною безпекою посилюється в умовах сучасних викликів, коли вивчаємо широке впровадження хмарних технологій, блокчейн-рішення, штучний інтелект в публічному адмініструванні та масову

цифровізацію даних. Як підкреслюється у звітах ООН, саме інформаційна безпека стає ключовою умовою формування відповідної цифрової довіри, без якої неможливе ефективне функціонування цифрового уряду [1, с. 9; 2, с. 15; 3, р. 143; 4]. Попри наявність зазначених досліджень, окремі аспекти цієї проблематики залишаються недостатньо розробленими. Зокрема, не сформульовано наразі цілісну концепцію інформаційної безпеки в е-урядуванні за умов військових дій та цифрової вразливості держави. Відповідно відкритими залишаються питання щодо розробки та апробації нових підходів до моделі імплементації міжнародного досвіду в українському контексті, з урахуванням правових, інституційних і технічних особливостей. Також потребує визначення напрямів подальшого розвитку електронного урядування на коротко-, середньо- і довгострокові горизонти планування. Таким чином, тема дослідження є актуальною як у теоретичному, так і в прикладному аспекті, відповідає стратегічним пріоритетам державної політики цифрової трансформації сьогодення та має потужний потенціал для практичного впровадження результатів дослідження в органах публічної влади та місцевого самоврядування.

Аналіз останніх досліджень і публікацій. Базові аспекти у сфері публічного управління та врядування, здобутки дослідження публічного управління господарською системою загалом та розвитком територіальних громад, побудова дослідницьких підходів до вивчення інформаційної безпеки та забезпечення інституцій електронного урядування створили еволюцію змін у працях як зарубіжних так і вітчизняних вчених [1, с. 7; 2, с. 15; 3, р. 143; 4]. Можна відзначити важливий доробок у формуванні теорії та методології вироблення публічної політики е-урядування, застосуванні підходів щодо організації діяльності органів публічної влади у цій сфері. Незважаючи на значну кількість вчених та їх праць [8, с. 57] щодо публічного управління, цифрового розвитку, питань місцевого самоврядування, інклюзивного місцевого розвитку досі не розроблено ґрунтовні базові підходи щодо процесу вдосконалення алгоритмів системи інформаційної безпеки та публічного управління в Україні, що ставить питання для вирішення.

Постановка завдання. Мета статті – теоретико-методологічне обґрунтування модернізації системи публічного управління інформаційної безпеки та модернізації публічного управління в Україні.

Виклад основного матеріалу. Розвиток країни безпосередньо залежить від зовнішніх умов всіх сфер життєдіяльності, оскільки саме вони створюють підґрунтя національної дії суспільства. Уряди світових держав стикаються з питаннями та проблемами, пов'язаними з адаптацією своїх національних моделей розвитку до сучасних вимог часу, пошуку актуальних дієвих моделей ефективного публічного управління, врядування задля забезпечення визначеного рівня урядування та належного рівня добробуту громадян. Трансформаційні процеси та вплив війни, що відбуваються в Україні також вимагають нових конструктивних рішень [8, с. 57] щодо створення ефективної системи органів публічної влади та врядування всіх рівнів в умовах е-урядування та цифровізації суспільства, що зумовлює використання механізму інформаційної безпеки на рівні територіальних громад та держави загалом.

Проблематика інформаційної безпеки є особливо актуальною в умовах активного розвитку інформаційного суспільства та поширення цифрових технологій, особливо у сфері електронного урядування [7]. За сучасними підходами інформаційна безпека трактується як комплексний стан захищеності інформаційного середовища держави, при якому гарантується конфіденційність, цілісність і доступність інформації, а також її надійний захист від внутрішніх і зовнішніх загроз [2, с. 119; 3, с. 148; 4, с. 14; 7]

Розуміння інформаційної безпеки в державному управлінні на сьогодні виходить далеко за межі традиційного уявлення про технічний захист. Воно охоплює широкий спектр заходів (від оновлення інформаційної інфраструктури до правового регулювання, від протидії кіберзагрозам до етичного управління персональними даними) та вимагає комплексного, міждисциплінарного підходу до формування належної національної політики у сфері інформаційної безпеки. Зарубіжний досвід надає підстави вважати, що забезпечення інформаційної безпеки в електронному урядуванні потребує цілісного та комплексного підходу, який охоплює не лише технічні аспекти, а й організаційні і правові аспекти [7].

За умов прогресивної цифровізації публічного управління та адміністрування фокусуються нові зрушення та зміни, що вимагають від уряду переосмислення підходів до вивчення інформаційної безпеки, пристосування до традиційних алгоритмів та структурних схем захисту інформації при врахуванні сучасних технологічних реалій (рис. 1).



Рис. 1. Структура інформаційної безпеки в системі е-урядування

З урахуванням наукового підґрунтя, деталізації можливих загроз, а також аспектів та рис правового, технічного та організаційного захисту, можна вважати, що безпека інформації має бути системно включена в архітектуру електронного урядування. Робочий алгоритм системної дії (рис. 2) є основою для подальшої оцінки моделі організації та проектування управлінських дій інформаційної безпеки.

Регіони нашої держави відіграють важливу роль у цифровій трансформації публічного управління та адміністрування, адже значна частина електронних послуг надається на місцевому рівні через органи місцевої влади та окремі територіальні громади. Реформа децентралізації розширила повноваження громад, що створило передумови для продуктивного впровадження цифрових рішень на місцях. Попри загальну позитивну динаміку, на сьогодні залишається

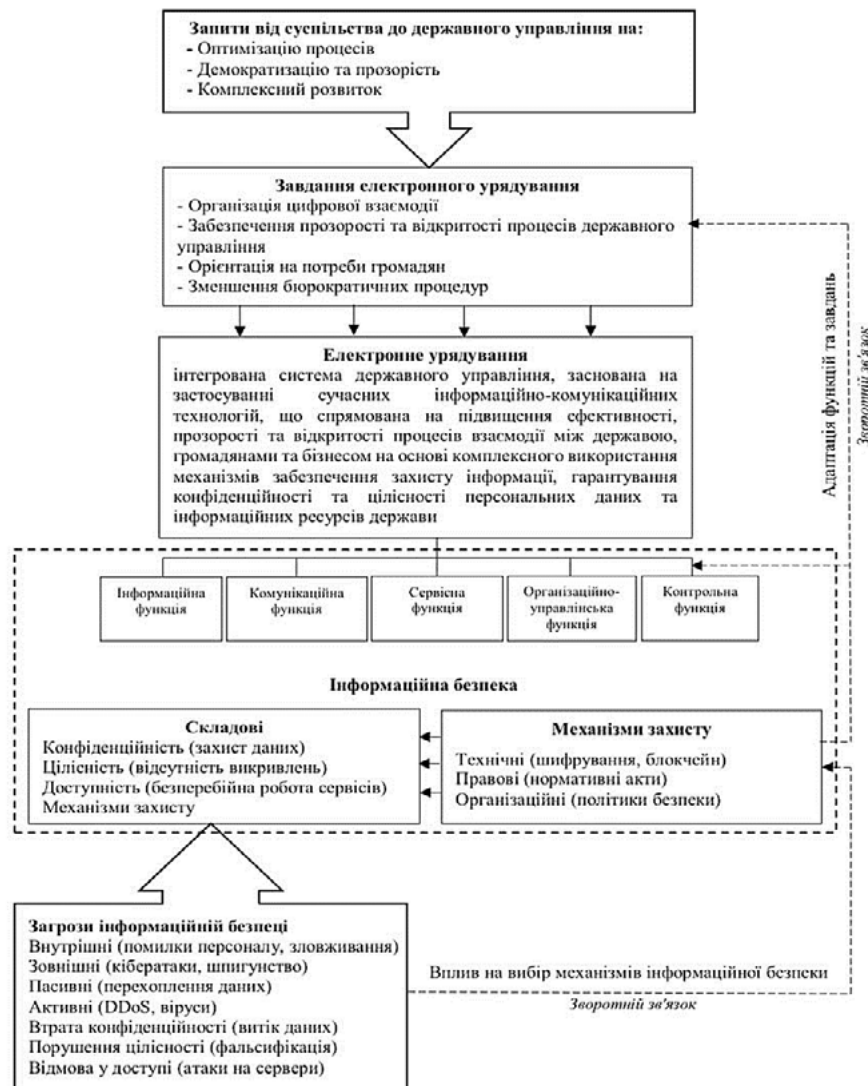


Рис. 2. Алгоритм системного взаємозв'язку е-урядування та інформаційної безпеки

проблема цифрового розриву між різними регіонами та соціальними групами, що підсилюється військовими діями з 2022 року. Згідно проведених досліджень, доступ до якісного інтернет-зв'язку та сучасних технологій суттєво різниться залежно від географії [7]. У віддалених селах Карпат, на прифронтових територіях доступ до широкосмтового інтернету все ще обмежений, що знижує можливість користуватися електронними послугами на рівні з мешканцями міст. Війна ще більше загострила проблеми нерівномірного доступу. У 2022 році через бойові дії і окупацію окремих територій багато хто втратив доступ до державних електронних сервісів [7].

Для успішної цифрової трансформації актуальним та необхідним є налагодження взаємодія між центральною владою та місцевими територіальними громадами. В Україні на сьогодні формується модель, коли уряд впроваджує роль стратега і координатора, а територіальні громади виступають безпосередніми виконавцями та джерелом зворотного зв'язку. Така подвійна комунікація дає можливість відформувати впровадження цифрової політики за місцевими потребами, створити

перспективність рішень і водночас врахувати особливості кожного регіону. Зростання рівня довіри громадян в суспільстві через забезпечення безпеки інформації є належною умовою достатньої цифрової трансформації державної влади [4, с. 12; 7].

Ми вважаємо за необхідне здійснити змістовне пояснення перспективних напрямів змін вивчення системи е-урядування за часовими лагами. Необхідність розробки довгострокових напрямів розвитку системи електронного урядування в Україні саме за такою схемою застосовується вченими в дослідницьких проробках [7] та починає працювати з необхідності створення послідовної, чітко вираженої і деталізованої політики сьогодення, яка здатна конструктивно аргументувати поставлені першочергові питання та виклики безпеки інформації. Використання засад та векторів, заснованих на розподілі конструктивних напрямів на часову перспективу, уможлиблює градацію всіх цілей і завдань за пріоритетами, ресурсною підтримкою та адаптації структури інститутів публічного управління до їх здійснення.

Короткочасні міри (1–2 роки) направлені на вирішення найбільш загострених проблем та опе-

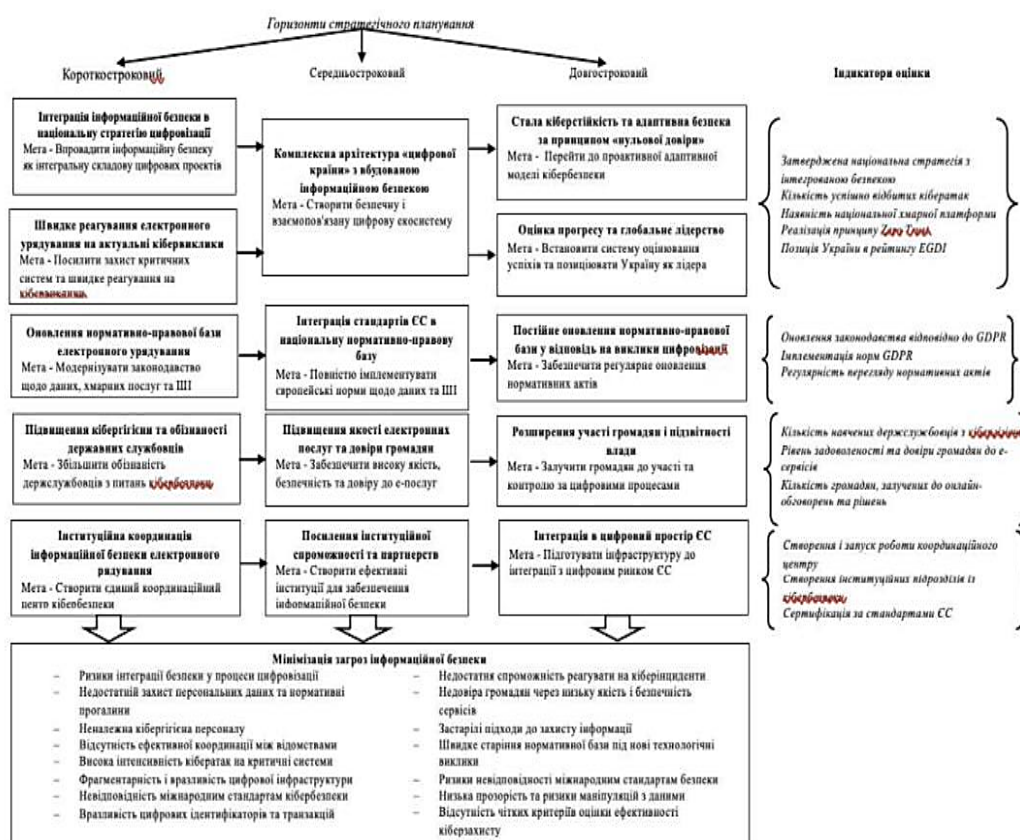


Рис. 3. Механізм розвитку системи е-урядування в умовах забезпечення інформаційної безпеки

Джерело: запропоновано автором за [4; 6]

ративну реакцію на найбільш необхідні виклики, пов'язані, зокрема, з кібербезпекою і впровадженням мінімально необхідних регуляторних змін, і це основа для подальшого розвитку та стабілізації питання, сприяючи формуванню довіри до електронних сервісів серед всіх громадян і бізнесу.

Середньочасова ситуація (3-5 років) сфокусована на структурні зміни, застосування новітніх технологій та законодавчі адаптації, що вимагають тривалого часу для здійснення, коли працює системне узгодження нормативних актів із міжнародними стандартами та європейськими базовими законами, має місце масштабна інституційна перебудова, може бути побудована єдина архітектура цифрових державних послуг з вбудованою системою інформаційною безпеки. І цей період є критично актуальним для зміцнення довіри населення і досягнення перспективних наслідків в рамках цифровізації держави.

Довгострокова ланка (часовим лагом понад 5 років) враховує стратегічні виклики та технологічні тренди, які неможливо реалізувати швидко, оскільки це потребує значних інвестицій, формування нової інфраструктури та структурних змін підходів щодо користування цифровими технологіями, коли має сенс будова фундаменту стійкої системи інформаційної безпеки, реалізація масштабних трансформацій, що дозволяють країні інтегруватися у глобальний цифровий простір. Такий розподіл стратегічних напрямів за часовими горизонтами, на думку окремих вчених, формує методологію вивчення, оскільки надає поетапність та погодження у реалізації належних цілей е-урядування, дозволяє стримко реагувати на позови та наслідки, та конкретизувати окреслені фактори ефективності, результативності та відповідальності на відповідних ланках еволюції (рис. 3).

Загальними питаннями, які дають відповідь щодо характерних ознак сучасного етапу публічного управління, слід відзначити зниження рівня

ефективності політики держави через ускладнення прогнозування економічного стану та суттєву деформацію основних реакцій національної господарської системи на ендогенні та екзогенні складові [7; 8; 5, с. 143]. Модернізація механізмів публічного управління та місцевого самоврядування виступає одним із багатьох трендів сучасного розвитку як господарських систем, так і державної політики, але так і не створює позитивного потенціалу оновлення та виходу з кризи національної господарської системи. Окремі дослідники вважають за необхідне підкреслити не модернізаційні зміни структури, а саме реконструктивні [8; 5, с. 5], що є актуальним під час війни.

Висновки. Пропрацювавши оцінені виклики і досягнення, дійшли висновку, що потребують додаткових ґрунтовних досліджень конкретні напрями модернізації розвитку е-урядування. Водночас перспективність окреслених змін в значній мірі пов'язана з якістю чинного нормативно-законодавчого регулювання, яке має виявити не тільки суттєві ризики та актуальні позови у сфері інформаційної безпеки, так і залежність правової адаптації до нормативної бази країн ЄС, що потребує розробки практично орієнтованих рекомендацій щодо вдосконалення чинного нормативно-правового регулювання з урахуванням принципів е-урядування (кіберстійкості, відкритості, громадської участі) та підходів євроінтеграції. Суттєві виклики органів виконавчої влади урядового рівня та врядування на рівні громад полягають у створенні належних умов підтримки ситуації з метою застосування відповідних цифрових технологій, за допомогою яких слід формувати зовнішнє інклюзивне середовище. В цілому, правове врегулювання участі громадськості у сфері інформаційної безпеки має базуватися на засадах прозорості, відкритості, партисипативності й кооперації, що відповідають основі європейської моделі цифрової демократії.

Список літератури:

1. Валевський О. Л. Державна політика в Україні: методологія аналізу, стратегія, механізми впровадження: [монографія]. Київ : НІСД, 2001. 242 с.
2. Євсюкова О. В., Кузменкова К. С. Формування інституційно-правових засад протидії дезінформації в Україні. *Наукові перспективи*. 2024. № 10(52). С. 119–128. DOI: [https://doi.org/10.52058/2708-7530-2024-10\(52\)-119-128](https://doi.org/10.52058/2708-7530-2024-10(52)-119-128)
3. Лашук О. С., Лілікович П. В., Сенченко І. В. Шляхи удосконалення державних механізмів у сфері національної безпеки. *Публічне управління та адміністрування в Україні*. 2024. №42. С.147–150.
4. Кутова М. А. Модель стратегічного планування розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки. *Вісник Хмельницького національного університету. Серія: Економічні науки*, 2025. №3. С.12–16. [https://doi.org/10.31891/2307-5740-2025-342-3\(1\)-1](https://doi.org/10.31891/2307-5740-2025-342-3(1)-1)
5. Гриценко А. Реконструктивний економічний розвиток, зміст, основні напрями і вектор соціальної справедливості. *Економічна теорія*. 2016. № 4. С. 5–19.

6. Бермас А. Міжнародний досвід діджиталізації діяльності органів державної влади. *Аспекти публічного управління*. 2024. 12(4). С. 13–18. <https://doi.org/10.15421/152443>

7. Кутова М. А. Розвиток системи електронного урядування в контексті забезпечення інформаційної безпеки України : дис....доктора філософії за спец. 281 Публічне управління та адміністрування. Чернігів: НУ «Чернігівська політехніка», 2025. 156 с.

8. Шевченко О. О., Єршов В. О., Коростильова О. О. Механізм модернізації системи публічного управління в місцевих органах влади: інструменти аутсорсингу та інклюзії. *Таврійський науковий вісник*. 2023. № 5. С. 57–62.

Shevchenko O. O., Letenko V. V. MECHANISM OF E-GOVERNMENT DEVELOPMENT IN THE CONTEXT OF ENSURING NATIONAL INFORMATION SECURITY

The article presents the rationale for improving the algorithm for changing the e-government system in the context of ensuring the country's information security; analyses general aspects of e-government in the format of digital public administration; reveals the basis of e-governance as a multi-component system (taking into account technological, regulatory, institutional, social and information security components, etc.) in a comprehensive approach (systematicity and application of the basics of e-governance to digital transformation agreements); the basic principles of transparency, interactivity, accessibility, efficiency, security, and inclusiveness of e-governance are analysed and presented, providing a basis for the further evolution of digital interaction between the government and society; the functions of e-governance, the algorithm of the relationship between information security and e-governance are elaborated, provided that the level of application of security issues structurally covers community requests, functional exercises of e-governance, information protection models, as well as the structure and impact of cyber threats on protection elements; an analysis of the domestic regulatory and legislative framework for the creation of information security in the field of e-government has been carried out in order to identify the shortcomings of the current legislation and the need to adapt it to modern challenges; The nature of modern information security threats was revealed, and the main risks facing e-government in Ukraine were identified, which allowed for a deeper understanding of the issue in the context of war. Strategic directions for the evolution of e-government in terms of information security were substantiated. A promising planning model was researched, based on a step-by-step analysis of strategic exercises for study. proposed improvements to the model for implementing state regional policy in the field of e-government through spatial structural changes to digital infrastructure, variable access to electronic services, regional risks at the level of territorial communities, and general threats to information security.

Key words: modernisation, local self-government, public administration, e-government, information.

Дата надходження статті: 29.10.2025

Дата прийняття статті: 20.11.2025

Опубліковано: 29.12.2025