

УДК 351:004

DOI: <https://doi.org/10.31470/2786-6246-2025-14-17-26>

Бут Юрій, кандидат економічних наук
Інституту держави і права ім. В.М. Корецького
НАН України

But Yurii, PhD in Economics at V.M. Koretsky
Institute of State and Law of National Academy
of Sciences of Ukraine

ORCID ID: <https://orcid.org/0009-0003-8256-6058>

ВІД ІНФРАСТРУКТУРИ ДО ІННОВАЦІЙ: ПРОБЛЕМИ ТА ВИКЛИКИ, З ЯКИМИ СТИКАЄТЬСЯ ВПРОВАДЖЕННЯ ЦИФРОВИХ ТРАНСФОРМАЦІЙ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

FROM INFRASTRUCTURE TO INNOVATION: PROBLEMS AND CHALLENGES FACED BY THE IMPLEMENTATION OF DIGITAL TRANSFORMATIONS IN PUBLIC ADMINISTRATION IN UKRAINE

Анотація. Стаття присвячена комплексному аналізу проблем і викликів, що супроводжують впровадження цифрових трансформацій у сфері публічного управління в Україні. У дослідженні наголошується, що цифровізація державного сектору є системним процесом, який вимагає наявності розвиненої інфраструктури, узгоджених нормативно-правових рамок, сучасних управлінських підходів та відповідного рівня компетентності державних службовців в роботі з цифровими інструментами. На основі огляду актуальних досліджень і нормативних ініціатив окреслено ключові тенденції розвитку цифрової держави та визначено специфічні передумови, притаманні українському контексту, включно з впливом повномасштабної війни на стійкість цифрових інфраструктур.

У роботі виділено п'ять основних груп бар'єрів, що сповільнюють цифрову модернізацію: технологічні та інфраструктурні обмеження, інституційно-правові диспропорції, проблеми управлінської культури, ризики кібербезпеки та виклики, пов'язані з глобальними технологічними трендами. Підкреслено їх взаємозалежність та комплексний характер, що потребує узгоджених і довгострокових стратегічних рішень. Окрему увагу приділено тому, як сучасні інноваційні процеси змінюють логіку функціонування державних інституцій, зумовлюючи потребу переходу від базової цифровізації до створення справді інноваційних, даних-орієнтованих і людиноцентричних сервісів.

Стаття містить пропозиції щодо стратегічних підходів до подолання виявлених бар'єрів, які включають розвиток інфраструктури, модернізацію нормативно-правового поля, посилення кіберстійкості, підвищення управлінської компетентності, а також розширення партнерств між державою, бізнесом та міжнародними організаціями. Підсумовано, що системне впровадження цих підходів здатне забезпечити формування стійкої та інноваційної цифрової екосистеми, необхідної для подальшої модернізації публічного управління.

Ключові слова: цифрова трансформація; публічне управління; цифрова інфраструктура; інституційні бар'єри; кібербезпека; інтероперабельність; технологічні тренди; державні цифрові сервіси; прийняття рішень на основі даних.

Abstract. The article is devoted to a comprehensive analysis of the problems and challenges that accompany the implementation of digital transformations in the field of public administration in Ukraine. The study emphasizes that the digitalization of the public sector is a systemic process that requires a developed infrastructure, an agreed regulatory framework, modern management approaches and an appropriate level of competence of civil servants in working with digital tools. Based on a review of current research and regulatory initiatives, key trends in the development of the digital state are outlined and specific prerequisites inherent in the Ukrainian context are identified, including the impact of a full-scale war on the stability of digital infrastructures.

The paper identifies five main groups of barriers that slow down digital modernization: technological and infrastructural limitations, institutional and legal imbalances, problems of managerial culture, cybersecurity risks and challenges associated with global technological trends. Their interdependence and complex nature are emphasized, which requires coordinated and long-term strategic decisions. Particular attention is paid to how modern innovation processes change the logic of the functioning of state institutions, causing the need to transition from basic digitalization to the creation of truly innovative, data-oriented and human-centric services.

The article contains proposals for strategic approaches to overcoming the identified barriers, which include infrastructure development, modernization of the regulatory and legal field, strengthening cyber resilience, increasing managerial competence, as well as expanding partnerships between the state, business and international organizations. It is concluded that the systematic implementation of these approaches can ensure the formation of a sustainable and innovative digital ecosystem necessary for the further modernization of public administration.

Keywords: digital transformation; public administration; digital infrastructure; institutional barriers; cybersecurity; interoperability; technological trends; government digital services; data-driven decision-making.

Постановка проблеми. Цифрова трансформація сфери публічного управління в Україні набула системного характеру та стала одним із визначальних факторів модернізації державного сектору, особливо в умовах воєнної агресії та необхідності забезпечення стійкості критичних державних функцій.

Незважаючи на значні успіхи – розвиток інтероперабельності державних реєстрів, масштабування електронних послуг, впровадження платформних рішень на зразок «Дії» – цифрова екосистема держави продовжує залишатися фрагментованою та нерівномірно розвиненою. Частина інформаційних систем функціонує на застарілій інфраструктурі, що обмежує швидкість, безпеку й можливість їх подальшої інтеграції. Поряд із цим, проблемним залишається питання якості даних, відсутність уніфікованих стандартів управління ними та недостатній рівень міжвідомчої координації, що уповільнює створення єдиного цифрового середовища.

Комплекс нормативно-правових актів, покликаних регулювати цифрові трансформації, часто відстає від реальних темпів технологічних змін, що створює правову невизначеність і ускладнює імплементацію інноваційних рішень. Додатковим викликом є кадровий дефіцит у сфері цифрових компетенцій, нерівномірний рівень цифрової готовності органів влади та обмеженість фінансових ресурсів, особливо на місцевому рівні. Кіберзагрози, посилені воєнними обставинами, формують окрему групу ризиків, що потребує комплексного реагування та переосмислення підходів до захисту державних інформаційних ресурсів.

У підсумку, перехід від цифровізації як технічного оновлення до побудови інноваційних, даних-орієнтованих моделей публічного управління стикається з низкою структурних і організаційних бар'єрів. Виявлення цих бар'єрів, визначення їх природи та наслідків є необхідним для формування ефективної політики цифрових трансформацій, здатної забезпечити стійкість та інноваційний розвиток державного сектору.

Мета дослідження полягає у визначенні та систематизації ключових проблем, бар'єрів та ризиків, що стримують ефективне впровадження цифрових трансформацій у сфері публічного управління України, а також у формулюванні аналітичних висновків щодо умов, механізмів і управлінських підходів, необхідних для переходу від базової цифровізації державних процесів до впровадження інноваційних, стійких та даних-орієнтованих моделей державного управління.

Аналіз останніх досліджень і публікацій. Питання цифрової трансформації публічного управління активно розробляється як у вітчизняній, так і в міжнародній науковій та аналітичній літературі. Українські дослідники наголошують на важливості інституційної спроможності, удосконалення управління даними та модернізації державної ІКТ-інфраструктури як ключових умов формування цифрової держави. У працях, присвячених е-урядуванню, підкреслюється необхідність

забезпечення інтероперабельності державних реєстрів, підвищення прозорості управлінських процесів, а також розвитку нормативно-правової бази, здатної підтримувати впровадження інноваційних рішень.

Окрему увагу в сучасних дослідженнях приділено впливу воєнних умов на еволюцію державних цифрових сервісів в Україні. Наголошується, що екстремальні обставини прискорили впровадження низки цифрових рішень, водночас загостривши проблеми кіберзахисту, стійкості інфраструктури та координації між суб'єктами публічного управління.

Значний внесок у дослідження проблематики роблять міжнародні організації. OECD, Світовий банк, UNDP та Європейська комісія акцентують увагу на тому, що цифрова трансформація вимагає не лише технологічних інвестицій, але й глибоких організаційних змін, переорієнтації державних інституцій на роботу з даними, формування культури сервісності та підвищення компетентності персоналу у сфері цифрових технологій [11; 12].

У звітах ЄС та ініціативи EU4Digital особливе місце займає питання сумісності державних систем, гармонізації стандартів безпеки та створення єдиного цифрового простору, що відповідає практикам країн ЄС [8; 10].

Попри широку представленість тематики, значна частина досліджень залишається зосередженою на окремих аспектах – правових, технологічних або організаційних. У той же час комплексний аналіз проблем та викликів, що перешкоджають переходу від базової цифровізації до інноваційного розвитку публічного управління в Україні, потребує подальшого узагальнення та систематизації.

Виклад основного матеріалу дослідження. Цифрова трансформація публічного управління розгортається на основі складного поєднання технічних, організаційних та соціальних чинників, що визначають можливості й темп модернізації державних інституцій. Універсальним для більшості країн є той факт, що цифровізація – це не лише технічне оновлення інструментів, а глибока системна зміна логіки управління, яка потребує зрілої інфраструктури, розвиненої культури взаємодії між установами та здатності швидко адаптуватися до технологічних змін. Через стрімку динаміку розвитку ІКТ державні системи майже завжди опиняються в ситуації, коли технології змінюються швидше, ніж процедури, регулювання чи організаційні моделі. Це створює природну інституційну інерцію, що ускладнює інтеграцію інновацій навіть у розвинених країнах.

Однією з ключових передумов є наявність сучасної цифрової інфраструктури – телекомунікаційних мереж, центрів обробки даних, державних реєстрів, платформ інтероперабельності [3]. Саме вони формують технічний каркас, від якого залежить можливість масштабування електронних сервісів, забезпечення їхньої безперервності та стійкості до збоїв. У глобальному контексті цифровізація завжди передбачає інтеграцію великої кількості роз'єднаних інформаційних систем, що виникали протягом тривалого часу та були створені під різні управлінські задачі. Тому майже скрізь спостерігається проблема фрагментації баз даних, несумісності форматів, відсутності єдиних стандартів обміну інформацією.

Для України ці загальносвітові тенденції мають додаткове забарвлення, обумовлене історією розвитку державних ІКТ-рішень та особливостями адміністративної системи. Протягом багатьох років державні органи розвивали власні реєстри й інформаційні системи автономно, що призвело до значної різноманітності технологічних платформ, різного рівня захищеності та неоднакової якості даних. Відсутність повної інтегрованості між ключовими реєстрами ускладнює ефективну роботу електронних сервісів, збільшує навантаження на громадян і бізнес, а також створює додаткові вимоги до державних органів щодо перевірки та синхронізації даних.

Окремим чинником, що суттєво впливає на передумови цифрової трансформації, є тривалий воєнний стан. Повномасштабна війна загострила проблеми фізичної стійкості ІТ-інфраструктури, спричинила потребу у швидкому резервуванні даних, перенесенні критичних реєстрів у хмарні середовища, підвищенні вимог до кіберзахисту. У таких умовах цифровізація державних послуг стала не лише інструментом модернізації, а й необхідним елементом забезпечення безперервності

управління [4]. Водночас війна прискорила певні процеси, сприяючи активнішій координації між установами та пришвидшенню прийняття рішень у сфері розвитку державних цифрових платформ.

Отже, інфраструктурні передумови цифрової трансформації в Україні визначаються поєднанням глобальних закономірностей та національних особливостей. Їхнє розуміння є необхідним етапом для аналізу проблем і викликів, які виникають уже на рівні практичної реалізації цифрових рішень, а також для формування цілісного підходу до модернізації державного управління.

Розвиток цифрових трансформацій у сфері електронних комунікацій відбувається в умовах дії низки системних обмежень, які формують складне середовище для планування, імплементації та масштабування державних політик. Аналіз проекту Стратегії розвитку сфери електронних комунікацій України до 2030 р. засвідчує, що ключові бар'єри згруповані у кілька взаємопов'язаних блоків, кожен з яких впливає на загальний темп модернізації галузі та її готовність до інтеграції в європейський цифровий простір [7].

Першою і найбільш очевидною групою викликів є **технологічні та інфраструктурні обмеження**, пов'язані з нерівномірністю покриття мережами фіксованого і мобільного зв'язку, зношеністю частини телекомунікаційної інфраструктури та недостатнім рівнем готовності до впровадження інноваційних рішень, таких як 5G, мережі нового покоління (NGA) чи програмно-визначені мережі (SDN/NFV).

Природа цих викликів пов'язана, насамперед, із нерівномірністю розвитку телекомунікаційної інфраструктури, значним ступенем зношеності частини мережевих елементів, використанням застарілого обладнання та різним рівнем технологічної готовності операторів до впровадження сучасних мережевих рішень. Додатковим чинником виступає вплив широкомасштабної військової агресії, що спричинила руйнування об'єктів критичної комунікаційної інфраструктури в багатьох регіонах країни, суттєво підвищивши вартість і складність їх відновлення.

Наслідки технологічних та інфраструктурних обмежень проявляються у зниженні якості послуг зв'язку, нерівному доступі користувачів до швидкісних мереж, сповільненні цифровізації державних сервісів та бізнес-процесів. Обмежена пропускна здатність мереж та недостатнє покриття фіксованим широкопasmовим Інтернетом стримують розвиток електронних послуг, дистанційної освіти, хмарних рішень і цифрових платформ взаємодії між державою та громадянами. Водночас запровадження технологій наступних поколінь, зокрема 5G, оптичних мереж з архітектурою FTTH, систем edge-computing чи програмно-визначених мереж (SDN/NFV), відбувається повільно, оскільки вимагає значних інвестицій, модернізації активного та пасивного обладнання, а також готовності операторів до масштабного оновлення інфраструктури.

Приклади цих бар'єрів є системними. У низці громад сільської місцевості досі спостерігається недостатній рівень покриття мобільним зв'язком четвертого покоління, що унеможлиблює доступ до сучасних цифрових сервісів для значної частини населення. Значна частина телекомунікаційних споруд, побудованих у 1990–2000-х рр., потребує модернізації або повної заміни, що є фінансово обтяжливим для операторів, особливо в умовах війни. Окремою проблемою є руйнування волоконно-оптичних ліній зв'язку в прифронтових регіонах, що вимагає термінового резервування маршрутів і створення альтернативних каналів передачі даних. Також простежується дефіцит енергетичної автономності мережевих вузлів, що проявляється у зниженні стійкості сервісів у періоди масованих атак на енергетичну інфраструктуру.

У сукупності технологічні та інфраструктурні обмеження формують критичний бар'єр для реалізації довгострокових завдань цифрової трансформації. Їх подолання потребує системної модернізації обладнання, підтримки операторів у впровадженні сучасних технологій, а також інвестицій у побудову стійких, масштабованих і захищених мереж електронних комунікацій, здатних забезпечувати безперервність сервісів навіть за умов високої турбулентності зовнішнього середовища.

Другою групою бар'єрів виступають **інституційно-правові диспропорції**, що включають фрагментарність нормативної бази, різні рівні відповідальності та повноважень між органами

влади, затримки в імplementації вторинного законодавства та обмеженість механізмів міжвідомчої координації. Значна частина регуляторних норм досі не забезпечує повного узгодження з правом Європейського Союзу, зокрема у частині доступу до інфраструктури, конкуренції на ринку та захисту прав кінцевих користувачів. Це уповільнює запровадження нових моделей управління електронними комунікаціями і створює правову невизначеність для бізнесу.

Головна сутність даної групи чинників полягає у взаємній невідповідності між темпами розвитку цифрових технологій та швидкістю оновлення нормативно-правової бази, інституційних процедур і формалізованих управлінських практик [5]. Чинне законодавство часто виявляється фрагментованим, з надмірною кількістю підзаконних актів, що дублюють або суперечать один одному, а окремі норми не враховують специфіку сучасних технологічних процесів – від електронної ідентифікації й обміну даними до управління реєстрами та кібербезпеки.

Негативні наслідки цих диспропорцій проявляються у затримках ухвалення рішень, неузгодженості між органами влади, правовій невизначеності та зниженні інституційної ефективності. За умов, коли регуляторне середовище не відповідає реальним потребам розвитку цифрових сервісів, державні органи вимушені імпровізувати або застосовувати застарілі процедури, що сповільнює впровадження інновацій і створює ризики помилок. Додаткову складність становить обмежена гнучкість правової системи, яка часто тяжіє до жорстких формальних вимог, у той час як цифрові технології потребують адаптивних, ризик-орієнтованих та процесно-орієнтованих механізмів регулювання.

Можна навести численні приклади таких інституційно-правових бар'єрів. Зокрема, затримки у впровадженні комплексного підходу до інтероперабельності реєстрів призводили до фрагментації інформаційних ресурсів та різних стандартів даних у відомствах. В окремих випадках законодавчі норми щодо електронної взаємодії між органами влади залишалися нечіткими або вимагали повторної паперової фіксації, що нівелює переваги цифровізації. Складності виникають і у сфері впровадження електронних довірчих послуг: відсутність достатньої гармонізації із європейськими стандартами eIDAS затримувала інтеграцію української інфраструктури електронної ідентифікації з європейським простором цифрових послуг [10].

Як і у випадку технологічних та інфраструктурних обмежень, важливим чинником є й вплив воєнного стану на інституційно-правовий контекст. З одного боку, він сприяв появі інноваційних рішень та дерегуляційних підходів, які дозволили оперативно запроваджувати нові цифрові сервіси. З іншого – значна кількість тимчасових норм, спрощених процедур і швидких регуляторних змін створюють ризик накопичення правової нестабільності, що може ускладнити подальшу систематизацію нормативного середовища.

У підсумку інституційно-правові диспропорції підривають сталість та передбачуваність цифрових трансформацій, ускладнюючи планування, координацію та інвестиції в інноваційні рішення. Подолання цих бар'єрів потребує гармонізації законодавства, впровадження всеохопних стандартів цифрової взаємодії, зміцнення ролі координуючих органів і запровадження принципів адаптивного регулювання, здатного оперативно реагувати на динаміку технологічного розвитку.

Третій блок бар'єрів охоплює **ризики кібербезпеки та захисту даних**, які суттєво зростають через одночасне розширення цифрового середовища та активізацію кібератак з боку держави-агресора. Система реагування на інциденти потребує подальшого посилення, зокрема на рівні координації між державними структурами та приватними операторами. Значним викликом залишається й забезпечення стійкості мереж, створення резервних маршрутів та підвищення захищеності критичної інфраструктури від комплексних загроз.

Ризики кібербезпеки та захисту даних є однією з найбільш критичних груп викликів, що визначають стійкість та надійність цифрових трансформацій у сфері публічного управління [1]. Їхня сутність становить поєднання зовнішніх загроз – з боку держав-агресорів, організованих хакерських угруповань та кіберзлочинності – із внутрішніми вразливостями державних інформаційних систем, інституційної культури та інфраструктури обробки даних. Умови воєнного стану різко посилили ці ризики, оскільки Україна фактично перебуває під постійним цифровим тиском, що поєднує DDoS-

атаки, спроби зламів реєстрів, компрометацію облікових записів та спроби викрадення критичних масивів даних.

Наслідки кіберзагроз є численними та багатовимірними. Злам або виведення з ладу державних цифрових сервісів знижує доступність базових адміністративних функцій, ускладнює роботу органів влади, призводить до простоїв та фінансових втрат. Компрометація персональних даних громадян підриває довіру до держави як до адміністратора інформаційних ресурсів, створює ризики шахрайства і посилює суспільну вразливість. У стратегічному вимірі атаки на реєстри або критичну комунікаційну інфраструктуру можуть мати наслідки для національної безпеки, порушуючи роботу оборонних, логістичних або гуманітарних систем.

Небезпечні інциденти в сфері кібербезпеки українських державних систем у 2022–2024 рр. показали, що зловмисники намагаються отримати доступ до реєстрів, модифікувати їх вміст або знищити критично важливі дані. Частими є атаки на поштові служби та внутрішні корпоративні системи органів влади, що використовують фішинг, соціальну інженерію або викрадення службових облікових записів. Значний виклик становить і неоднорідність рівня захищеності інформаційних ресурсів: деякі відомства впровадили сучасні засоби кіберзахисту, багатфакторну автентифікацію та системи моніторингу інцидентів, тоді як інші продовжують працювати на застарілих платформах, що мають низку відомих вразливостей [4].

Внутрішні чинники також суттєво впливають на рівень ризику. Недостатня кіберграмотність працівників, слабка культура управління доступами, несистемне резервування даних і відсутність єдиних стандартів інформаційної безпеки ускладнюють захист державних систем. У низці випадків підвищена вразливість виникає через недостатній контроль над сторонніми підрядниками або через фрагментацію ІТ-ландшафту, коли різні органи влади застосовують несумісні або застарілі інструменти кіберзахисту.

Таким чином, ризики кібербезпеки та захисту даних формують комплексний бар'єр, що впливає на всі етапи цифрової трансформації – від проєктування цифрових сервісів до їх довгострокового функціонування. Їх подолання потребує системного підходу, що поєднує модернізацію інфраструктури, розвиток національних центрів кіберзахисту, підвищення компетентностей персоналу та впровадження єдиних стандартів інформаційної безпеки, які відповідають вимогам як воєнного часу, так і перспективного мирного розвитку.

Четверту групу негативних чинників становлять **кадрові та соціальні бар'єри**, пов'язані з дефіцитом висококваліфікованих ІКТ-фахівців, відтоком спеціалістів за кордон, недостатнім рівнем цифрових навичок користувачів і нерівним доступом до цифрових послуг між різними соціальними групами. Ці фактори безпосередньо впливають на темп упровадження інновацій, а також на здатність суспільства адаптуватися до нових моделей комунікацій та сервісів.

Проблеми управлінської культури та компетентності працівників є однією з найбільш складних та глибоко вкорінених груп бар'єрів, що впливають на успішність цифрових трансформацій у сфері публічного управління [2]. Їхня природа полягає у розриві між сучасною логікою цифрового врядування – гнучкою, даними-орієнтованою, сервісною – та традиційними управлінськими практиками, які сформувалися у добу паперового документообігу, жорстких вертикалей і нормативно-функціональної моделі діяльності державних органів. У результаті працівники нерідко демонструють готовність приймати цифрові інструменти формально, без зміни внутрішніх процесів, що перетворює цифровізацію на механічний перенос існуючих логік роботи в електронний формат.

Наслідки цих диспропорцій відчутні на багатьох рівнях. Низька цифрова зрілість управлінців та недостатні компетентності у сфері роботи з даними призводять до помилок у плануванні цифрових проєктів, неправильного визначення пріоритетів або вибору технологічних рішень, що не відповідають реальним потребам організації. Слабка культура командної взаємодії стримує розвиток міжвідомчої співпраці, яка є ключовою для інтеперабельності та комплексності державних послуг. Водночас недостатній рівень розуміння ризиків цифрової безпеки серед

працівників підвищує вразливість до кіберінцидентів та створює додаткові загрози для стабільності цифрових сервісів.

Практичні приклади таких бар'єрів можна спостерігати у численних ситуаціях: від нерегулярного оновлення даних у державних інформаційних системах до хибних підходів до автоматизації, коли процеси digital-by-default впроваджуються поверх старих адміністративних практик без їх реінжинірингу. Значна частина державних службовців використовує інформаційні системи як інструмент виконання формальних процедур, а не як середовище для аналітичного опрацювання даних чи прийняття управлінських рішень. Окремим проявом є недостатня культура проектного управління, що призводить до затримок у реалізації цифрових ініціатив, відсутності чітких критеріїв оцінювання ефективності та слабкої координації між стейкхолдерами.

Вплив війни лише підсилив ці аспекти: різке зростання навантаження на державний сектор, зміна пріоритетів та нестача кадрів загострили проблему нерівномірного рівня компетентності в роботі з інформаційними технологіями. З одного боку, виник попит на спеціалістів зі складними цифровими навичками, включно з управлінням даними, кібербезпекою, розробкою цифрових сервісів. З іншого – значна частина органів публічного управління не має достатнього кадрового ресурсу та можливостей для системного підвищення кваліфікації [2; 4].

Таким чином, проблеми управлінської культури, цифрової грамотності та недостатнього рівня кваліфікації формують комплексний бар'єр для розвитку цифрового врядування. Їх подолання вимагає не лише інвестування в навчання державних службовців, але й інституціоналізації нових управлінських практик: розвиток data-driven decision-making, поширення сервісного мислення, створення мотивуючого кадрового середовища, усунення культури «формального виконання» та впровадження механізмів постійного професійного розвитку.

Нарешті, як окрему групу чинників, що ускладнюють впровадження цифрових технологій в публічному управлінні, варто виділити **глобальні технологічні тренди та виклики**. Розвиток цифрових трансформацій в Україні відбувається в контексті стрімкої зміни глобального технологічного ландшафту. Поява нових інструментів, платформ і методів обробки даних відкриває значні можливості для модернізації публічного сектору, однак паралельно формує низку складних викликів, що потребують стратегічно виважених рішень. У цьому контексті важливо визначити ключові технологічні тренди, які вже впливають або найближчим часом впливатимуть на державне управління, а також окреслити пов'язані з ними ризики та бар'єри.

Одним із найбільш визначальних трендів є прискорене впровадження хмарних технологій. Для України це означає перехід від локальних інфраструктур до масштабованих, розподілених і більш надійних рішень, що забезпечують гнучкість, безперервність роботи систем та можливість швидкого реагування на зміни. Водночас такий перехід вимагає вирішення питань щодо правового режиму даних, вибору оптимальних моделей розгортання (public / hybrid cloud), забезпечення стійкості до кібератак та побудови належних механізмів контролю доступу [11].

Іншим важливим напрямом виступає розвиток штучного інтелекту та машинного навчання, які дедалі частіше застосовуються для аналітики великих масивів даних, прогнозування та підтримки прийняття рішень. Для публічного сектору це відкриває можливість створення систем раннього попередження, прогнозової аналітики у сфері соціальних політик, безпеки, логістики та управління ризиками. Проте водночас постає проблема алгоритмічної прозорості, етичних стандартів роботи з даними, ризиків упередженості моделей та відповідальності за наслідки автоматизованих рішень.

Значного поширення набувають також технології блокчейн, які вже використовуються для забезпечення незмінності записів, прозорості транзакцій та підвищення довіри в реєстраційних системах. Проте впровадження таких рішень вимагатиме стандартизації протоколів, визначення взаємодії між різними реєстрами та вирішення питань масштабованості, що залишається викликом для державних систем із великим навантаженням [11; 12].

Окрему групу трендів становлять також інструменти цифрової ідентичності й еволюція електронних довірчих послуг. Розвиток мобільної ідентифікації, біометрії та інтегрованих систем

eID дозволяє покращити доступ громадян до послуг і посилити їхню безпеку. Водночас упровадження таких рішень повинно супроводжуватися забезпеченням сумісності між різними системами, чітким правовим регулюванням і захистом персональних даних на всіх етапах ідентифікації.

Крім того, важливий вплив на формування політики у сфері цифрових трансформацій мають тренди автоматизації й роботизації, включно з RPA (Robotic Process Automation), які дозволяють оптимізувати рутинні управлінські процеси та зменшити навантаження на службовців. Виклик полягає у необхідності перегляду адміністративних процедур, підготовці кадрів та зниженні ризиків технологічної залежності від зовнішніх постачальників.

Таким чином, технологічні тренди створюють значні можливості для якісного оновлення системи публічного управління, але їх упровадження потребує комплексної та узгодженої політики, орієнтованої на баланс між інноваційністю, безпекою та інституційною стійкістю.

У комплексі зазначені групи викликів утворюють багатовимірну систему бар'єрів, що стримує потенціал цифрової трансформації та вимагає скоординованих рішень на державному, регіональному й корпоративному рівнях. Їх подолання неможливе без системного оновлення регуляторного середовища, розвитку інфраструктури, забезпечення кіберстійкості та формування кадрового потенціалу, здатного підтримувати динаміку змін.

Ефективна реалізація цифрових трансформацій у сфері публічного управління потребує системного подолання комплексних бар'єрів, що виникають на технологічному, інституційному, управлінському та безпековому рівнях. З огляду на масштабність і взаємозалежність викликів, стратегічні підходи мають ґрунтуватися на принципах узгодженості, довгостроковості та адаптивності до динамічних умов. Нижче окреслено ключові напрями, які формують цілісну рамку для подолання зазначених перешкод.

Безперечно, критичним напрямом є **інституційне укріплення та модернізація нормативно-правового середовища**, яке має забезпечити передбачуваність, єдність підходів та правову визначеність у сфері цифровізації. Йдеться про оновлення законодавства щодо електронної ідентифікації, обігу даних, кібербезпеки, а також про гармонізацію національних стандартів із європейськими. Важливо також забезпечити стабільність регуляторних політик, зменшивши фрагментацію та конфлікт норм, що гальмують розвиток платформних рішень і міжвідомчих інтеграцій.

Також важливим напрямом виступає **розвиток цифрової інфраструктури та технологічної спроможності держави**, що включає масштабування хмарних сервісів, модернізацію державних реєстрів, розвиток систем кіберзахисту, а також перехід до інтероперабельних архітектур. Важливим елементом є забезпечення рівномірної доступності цифрових послуг по всій країні, у тому числі в громадах, які постраждали від війни чи мають обмежені ресурси. Такі інвестиції створюють необхідну основу для стійкості цифрових процесів і кращої підготовленості до криз.

Ключовим фактором є також **підвищення управлінської культури та формування нових компетентностей державних службовців**. Реалізація цифрових трансформацій вимагає іншої логіки ухвалення рішень – орієнтованої на дані, відкритість, експериментальність та мультидисциплінарність. Тому важливо інвестувати у навчальні програми з цифрових навичок, управління даними, аналітики, кібергігієни, а також розвивати здатність працювати з інноваційними інструментами. Не менш важливим є підтримання культури співпраці та обміну знаннями між установами.

Стратегічну необхідність становить **посилення кіберстійкості та управління ризиками безпеки даних**. З огляду на високу інтенсивність кіберзагроз, цифрова трансформація має враховувати вимоги до захищеності критичних інформаційних ресурсів, побудову системи оперативного реагування, впровадження сучасних технологій моніторингу, логування та автентифікації у відповідності до стандартів ЄС [9]. Важливо також забезпечити наскрізну політику управління даними, яка включає чіткі ролі відповідальності, механізми контролю доступу та оцінку впливу на приватність.

Окремий напрям подолання викликів пов'язаний із **розвитком партнерських моделей**, що передбачають активну взаємодію держави з приватним сектором, науковими інституціями та міжнародними організаціями. Залучення таких партнерств сприяє поширенню інновацій, доступу до експертизи, отриманню ресурсів і технологій, які держава не завжди може створити власними силами. Особливу роль відіграють міжнародні проекти технічної допомоги, які допомагають впроваджувати сучасні стандарти, інструменти та методології.

Нарешті, важливим стратегічним підходом є **орієнтація на користувача та підвищення якості цифрових послуг**, що включає аналіз потреб громадян, тестування сервісів, спрощення процедур і скорочення бюрократичних бар'єрів. Такий підхід забезпечує довіру до цифрових рішень, сприяє їх масовому використанню та стимулює подальшу еволюцію цифрової держави.

У сукупності ці стратегічні напрями дозволяють сформувати комплексну та ефективну політику подолання бар'єрів цифрових трансформацій, яка враховує інституційні, технологічні, управлінські та соціальні чинники і закладає основу для створення цілісної, стійкої та інноваційної цифрової екосистеми України.

Висновки. Проведений аналіз дозволяє констатувати, що цифрова трансформація публічного управління в Україні є складним і багатовимірним процесом, який розгортається в умовах надзвичайно динамічного технологічного середовища та додаткових ризиків, спричинених війною. Водночас вона спирається на потужні інфраструктурні та інституційні передумови, сформовані протягом останніх років, що створює фундамент для модернізації державного управління та підвищення його ефективності.

Виявлені виклики структуровані у п'ять окремих груп: технологічні обмеження, інституційно-правові диспропорції, проблеми управлінської культури, ризики кібербезпеки та вплив глобальних технологічних трендів. Водночас наголошується, що незважаючи на різну природу викликів, вони існують не відокремлено, а мають переважно взаємопов'язаний характер і виступають системними бар'єрами на шляху цифровізації. Їхня природа пов'язана як із внутрішніми структурними недоліками сектору публічного управління, так і з зовнішніми чинниками, зокрема масштабною та динамічною діджиталізацією соціальної сфери на глобальному національному рівні, та повномасштабною війною проти України.

Успішне подолання цих бар'єрів можливе лише за умови реалізації комплексної державної політики, яка поєднує інституційне оновлення, розвиток інфраструктури, зміцнення кіберстійкості, підвищення кваліфікації державних службовців в роботі із сучасними інформаційними технологіями та інструментами й впровадження практик інноваційного управління. Особливої ваги набувають партнерські моделі взаємодії держави, приватного сектору та міжнародних організацій, здатні прискорити впровадження сучасних технологічних рішень та надати доступ до найкращих практик.

Перспективи подальших досліджень у цьому напрямі пов'язані з необхідністю глибшої оцінки ефективності цифрових інструментів, аналізом стійкості інфраструктурних рішень у кризових умовах, вивченням поведінкових аспектів користувачів цифрових послуг, а також розробкою моделей інтеграції інновацій у діяльність органів влади. Подальші наукові розвідки можуть також зосереджуватися на порівняльному аналізі міжнародного досвіду та можливостях його адаптації до українського контексту, що сприятиме формуванню більш зрілої, ефективної та людиноцентричної цифрової держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 12.07.2025).
2. Запорожець Т. Механізми публічного управління розвитком інтелектуального потенціалу в умовах цифровізації. Наукові перспективи. 2024. № 11(53). URL: <http://perspectives.pp.ua/index.php/np/article/view/17086/17158> (дата звернення: 12.07.2025).
3. Концепція розвитку електронного урядування в Україні: схвалена розпорядженням Кабінету Міністрів України від 20.09.2017 № 649-р. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text> (дата звернення: 12.07.2025).
4. Кучменко В., Ватульєв М. Цифрова трансформація публічного управління в умовах воєнного стану. *Молодий вчений*, 4 (135). URL: <https://doi.org/10.32839/2304-5809/2025-4-135-14> (дата звернення: 12.07.2025).

5. Наджафлі Е. Цифрова держава в контексті правової реформи в Україні: теоретико правовий аспект. *Право і безпека*. 2022. Вип. 32(85). С. 202–216. URL: <https://pb.univd.edu.ua/index.php/PB/article/download/628/482/> (дата звернення: 12.07.2025).
6. Національна економічна стратегія до 2030 року: затверджена постановою Кабінету Міністрів України від 03.03.2021 № 179. URL: <https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text> (дата звернення: 12.07.2025).
7. Стратегія розвитку сфери електронних комунікацій України до 2030 року. Міністерство цифрової трансформації України. URL: <https://www.kmu.gov.ua/storage/app/uploads/public/684/1ae/cf6/6841aecf65db0391819424.pdf> (дата звернення: 12.07.2025).
8. Digital Decade Policy Programme 2030 (Decision (EU) 2022/2481 of the European Parliament and of the Council). European Commission. URL: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj> (дата звернення: 12.08.2025).
9. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555> (дата звернення: 12.07.2025).
10. EU4Digital Facility. Digital Regulation Support to Ukraine (DRS2UA). URL: <https://eufordigital.eu/discover-eu/digital-regulation-support-to-ukraine-drs2ua/> (дата звернення: 18.08.2025).
11. OECD. The Digital Government Policy Framework: Six dimensions of a Digital Government. Paris: OECD Publishing, 2020. URL: https://www.oecd.org/en/publications/the-oecd-digital-government-policy-framework_f64fed2a-en.html (дата звернення: 18.08.2025).
12. World Bank Group. World Development Report 2021: Data for Better Lives. Washington, DC: World Bank, 2021. 240 p. URL: <https://www.worldbank.org/en/publication/wdr2021> (дата звернення: 18.09.2025).

REFERENCES

1. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» vid 05.10.2017 №2163-VIII [Law of Ukraine On the Basic Principles of Ensuring Cybersecurity of Ukraine from October 05 2017, №2163-VIII]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19> [in Ukrainian].
2. Zaporozhets, T. (2024). Mekhanizmy publicnogo upravlinnia rozvytkom intelektualnogo potentsialu v umovakh tsyfrovizatsii [Mechanisms of public management of the development of intellectual potential in the conditions of digitalization]. *Naukovi perspektyvy – Scientific Perspectives*, № 11(53). Retrieved from <http://perspectives.pp.ua/index.php/np/article/view/17086/17158> [in Ukrainian].
3. Kontseptsiiia rozvytku elektronnoho uriaduvannia v Ukraini: skhvalena rozporiadzhenniam Kabinetu Ministriv Ukrainy vid 20.09.2017 № 649-p [Concept of e-Government Development in Ukraine: approved by the order of the Cabinet of Ministers of Ukraine from September 20 2017, №649-p]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text> [in Ukrainian].
4. Kuchmenko, V., & Vatuliyev, M. (2025). Tsyfrova transformatsiia publicnogo upravlinnia v umovakh voiennoho stanu [Digital transformation of public administration in conditions of martial law]. *Molodyi vchenyi – Young Scientist*, 4(135). Retrieved from <https://doi.org/10.32839/2304-5809/2025-4-135-14> [in Ukrainian].
5. Nadzhafli, E. (2022). Tsyfrova derzhava v konteksti pravovoi reformy v Ukraini: teoretyko pravovyi aspekt [Digital state in the context of legal reform in Ukraine: theoretical and legal aspect]. *Pravo i bezpeka – Law and Security*, 32(85), 202–216. Retrieved from <https://pb.univd.edu.ua/index.php/PB/article/download/628/482/> [in Ukrainian].
6. Natsionalna ekonomichna stratehiia do 2030 roku: zatverdzhena postanovoiu Kabinetu Ministriv Ukrainy vid 03.03.2021 № 179 [National Economic Strategy until 2030: approved by the Resolution of the Cabinet of Ministers of Ukraine from March 03 2021, №179]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text> [in Ukrainian].
7. Stratehiia rozvytku sfery elektronnykh komunikatsii Ukrainy do 2030 roku. Ministerstvo tsyfrovoy transformatsii Ukrainy [Strategy for the Development of the Electronic Communications Sector of Ukraine until 2030. Ministry of Digital Transformation of Ukraine]. *www.kmu.gov.ua*. Retrieved from <https://www.kmu.gov.ua/storage/app/uploads/public/684/1ae/cf6/6841aecf65db0391819424.pdf> [in Ukrainian].
8. Digital Decade Policy Programme 2030 (Decision (EU) 2022/2481 of the European Parliament and of the Council). European Commission. *eur-lex.europa.eu*. Retrieved from <https://eur-lex.europa.eu/eli/dec/2022/2481/oj> [in English].
9. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). EUR-Lex. *eur-lex.europa.eu*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555> [in English].
10. EU4Digital Facility. Digital Regulation Support to Ukraine (DRS2UA). *eufordigital.eu*. Retrieved from <https://eufordigital.eu/discover-eu/digital-regulation-support-to-ukraine-drs2ua/> [in English].
11. OECD. The Digital Government Policy Framework: Six dimensions of a Digital Government. Paris: OECD Publishing, 2020. *www.oecd.org*. Retrieved from https://www.oecd.org/en/publications/the-oecd-digital-government-policy-framework_f64fed2a-en.html [in English].
12. World Bank Group (2021). World Development Report 2021: Data for Better Lives. Washington, DC: World Bank. *www.worldbank.org*. Retrieved from <https://www.worldbank.org/en/publication/wdr2021> [in English].

Подано до редакції 22.09.25 р.

Прийнято до друку 24.10.25 р.