УДК 351:004.7:005.334
JEL H11, H83, O33, O38
DOI https://doi.org/10.32782/2786-765X/2026-15-13

Кириченко Г.В.
кандидат наук з державного управління,
завідувачка відділу аспірантури та докторантури,
ЗВО «Відкритий міжнародний університет
розвитку людини «Україна»
ORCID: https://orcid.org/0000-0003-1067-8758

РИЗИКИ ТА ВИКЛИКИ ВПРОВАДЖЕННЯ ЦИФРОВИХ ІННОВАЦІЙ У ДЕРЖАВНОМУ УПРАВЛІННІ: ОРГАНІЗАЦІЙНІ, ТЕХНОЛОГІЧНІ ТА КІБЕРБЕЗПЕКОВІ АСПЕКТИ

У статті досліджено ризики та виклики, що виникають у процесі впровадження цифрових інновацій у систему державного управління, з урахуванням організаційних, технологічних та кібербезпекових аспектів цифрової трансформації. Обґрунтовано, що цифровізація державного управління, поряд із підвищенням ефективності управлінських процесів, доступності публічних послуг, прозорості та оперативності прийняття рішень, формує нові джерела системних ризиків, здатних впливати на стійкість і безперервність функціонування публічних інституцій. Обґрунтовано доцільність комплексного механізму управління такими ризиками, що має поєднувати стратегічне планування цифрової трансформації, інституційну координацію, розвиток цифрових компетентностей, технологічну модернізацію, стандартизацію та інтероперабельність інформаційних систем, захист даних, кібербезпеку й безперервний моніторинг ризиків. Визначено, що ефективність цифрових інновацій у державному управлінні залежить від здатності держави не лише впроваджувати нові технології, а й забезпечувати їх безпечну, стійку, інституційно узгоджену та орієнтовану на суспільні потреби інтеграцію в систему публічного управління.

Ключові слова: цифрові трансформації, ризики, цифрові інновації, державне управління, кібербезпека, інновації, управління ризиками, цифрове врядування.

Постановка проблеми. Цифрова трансформація державного управління є важливим напрямом модернізації публічного сектору, що забезпечує підвищення ефективності управлінських процесів, доступності публічних послуг та якості взаємодії держави з громадянами. Водночас масштабне впровадження цифрових інновацій породжує нові ризики, пов'язані не лише з технологічними рішеннями, а й з організаційною готовністю державних інституцій та рівнем кібербезпеки.

Основними організаційними ризиками виступають інституційний опір змінам, недостатня міжвідомча координація, дефіцит цифрових компетентностей персоналу та фрагментарність цифрових перетворень. Технологічні ризики охоплюють несумісність інформаційних систем, застарілість цифрової інфраструктури, проблеми інтеграції державних реєстрів, технологічну залежність та недостатню якість даних. Водночас зростання цифрової залежності державних інституцій посилює кібербезпекові загрози, зокрема кібератаки, витоки даних, несанкціонований доступ і порушення безперервності функціонування критичних цифрових сервісів.

За таких умов проблема полягає у невідповідності між темпами впровадження цифрових інновацій та спроможністю державних інституцій своєчасно ідентифікувати й мінімізувати пов'язані з ними ризики. Це актуалізує необхідність формування комплексного підходу до управління організаційними, технологічними та кібербезпековими ризиками як взаємопов'язаними складовими цифрової трансформації державного управління.

Аналіз останніх досліджень і публікацій. Теоретичні та прикладні засади цифрової трансформації державного управління досліджували В. С. Куйбіда, О. В. Карпенко, В. В. Наместнік [1], які розкривають сутність цифрового врядування та його роль у модернізації публічного управління. Проблематику цифрових технологій як інструменту реінжинірингу державного управління досліджують Н. Костенюк, І. Макарова, Ю. Пігарєв та Л. Сметаніна [2]. Кібербезпековий аспект цифровізації представлений у працях І. Скляр [3], зокрема щодо сутності та змісту кібербезпеки, а також Ю. Богач [4] та Д. Заболотенко, К. Герасимюк [5], які досліджують організаційно-правові засади захисту критичної інформаційної інфраструктури.

© Кириченко Г.В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Водночас у наукових працях переважно розглядаються окремі аспекти цифрової трансформації та кібербезпеки, тоді як комплексне дослідження взаємопов'язаних організаційних, технологічних і кібербезпекових ризиків упровадження цифрових інновацій та механізмів їх системного управління залишається недостатньо розробленим, що визначає необхідність подальшого обґрунтування ризик-орієнтованого підходу до цифрової трансформації державного управління.

Мета статті. Метою статті є теоретичне обґрунтування та систематизація організаційних, технологічних і кібербезпекових ризиків упровадження цифрових інновацій у державному управлінні, а також визначення комплексних підходів до їх мінімізації та забезпечення стійкої й безпечної цифрової трансформації публічних інституцій.

Виклад основних матеріалу дослідження. Цифрова трансформація державного управління є системним процесом інституційної та технологічної модернізації публічного сектору, спрямованим на підвищення результативності управлінських рішень, оптимізацію адміністративних процедур, розширення доступності публічних послуг та поглиблення взаємодії держави із суспільством. Водночас масштабування цифрових технологій змінює не лише інструментарій державного управління, а й характер управлінських ризиків, оскільки критична залежність публічних інституцій від цифрової інфраструктури, інформаційних систем і даних формує нові джерела організаційної, технологічної та кібербезпекової вразливості. Зокрема, фрагментарність цифрових перетворень, недостатня інституційна координація, дефіцит цифрових компетентностей, технологічна несумісність інформаційних систем та недостатня захищеність державних інформаційних ресурсів можуть обмежувати очікуваний ефект від цифрових інновацій і створювати ризики порушення безперервності управлінських процесів. Особливого значення набуває й те, що взаємопов'язаність зазначених ризиків зумовлює їх кумулятивний характер: організаційні недоліки можуть посилювати технологічні вразливості, тоді як технологічні уразливості створюють додаткові передумови для реалізації кіберзагроз. Отже, результативність цифрової трансформації державного управління доцільно розглядати не лише крізь призму рівня технологічного впровадження, а передусім через спроможність публічних інституцій забезпечувати комплексне управління ризиками, технологічну стійкість, кібербезпеку та безперервність виконання державних функцій.

Доцільно відмітити, що цифровізація державного управління забезпечує автоматизацію адміністративних процедур, прискорення обробки інформації, підвищення оперативності управлінських рішень, доступності публічних послуг і прозорості діяльності органів влади. Водночас перенесення значної частини управлінських процесів у цифрове середовище посилює залежність публічних інституцій від надійності цифрової інфраструктури, інформаційних систем та якості даних, що зумовлює виникнення технологічних ризиків, пов'язаних із технічними збоями, несумісністю систем, втратою даних і порушенням доступності цифрових сервісів. Розширення цифрової інфраструктури одночасно збільшує кібернетичну вразливість державних інформаційних ресурсів до кібератак, несанкціонованого доступу та витоку даних. Додатковим джерелом ризиків виступають організаційні чинники, зокрема інституційний опір змінам, недостатня міжвідомча координація та дефіцит цифрових компетентностей персоналу [1].

Взаємопов'язаність організаційних, технологічних і кібербезпекових ризиків зумовлює їх системний та кумулятивний характер, за якого реалізація одного ризику може посилювати інші. Сукупний вплив таких ризиків здатний порушувати безперервність управлінських процесів, знижувати доступність публічних послуг та послаблювати інституційну спроможність держави. Тому ефективність цифровізації має оцінюватися не лише за рівнем технологічного впровадження, а й за здатністю публічних інституцій забезпечувати стійкість, безпеку та безперервність цифрових процесів, що це зумовлює необхідність комплексного ризик-орієнтованого підходу до управління цифровою трансформацією, спрямованого на своєчасну ідентифікацію, оцінювання та мінімізацію організаційних, технологічних і кібербезпекових загроз.

З огляду на те, що результативність цифрових інновацій залежить не лише від технологічної спроможності, а й від готовності публічних інституцій до організаційних та управлінських змін, доцільно систематизувати основні організаційні ризики цифрової трансформації та конкретизувати форми їх прояву [2]:

1. Інституційний опір змінам – пов'язаний зі збереженням усталених адміністративних практик, небажанням персоналу змінювати порядок виконання функцій та недостатньою готовністю керівництва до трансформації управлінських моделей. Практичним проявом такого ризику може бути формальне

впровадження систем електронного документообігу за одночасного збереження паперового дублювання документів, що нівелює очікуваний ефект цифровізації. Іншим прикладом є небажання працівників використовувати автоматизовані системи управління даними через побоювання зміни усталеного розподілу повноважень або контролю за результативністю їх роботи.

2. Недостатня координація між органами державної влади – проявляється у відсутності узгоджених підходів до цифровізації, дублюванні інформаційних ресурсів та обмеженому обміні даними між державними інституціями. Прикладом може бути функціонування інформаційних систем різних органів влади, які використовують несумісні формати даних і не забезпечують автоматизований обмін інформацією. Унаслідок цього громадянин або суб'єкт господарювання може бути змушений повторно подавати відомості, які вже наявні в іншому державному реєстрі.

3. Фрагментарність цифрової трансформації – виникає у випадках, коли цифрові рішення впроваджуються як окремі проєкти без належного взаємозв'язку із загальною архітектурою державного управління. Наприклад, окремий орган може створити власну електронну платформу для надання послуг, яка не інтегрована з іншими державними інформаційними системами та не використовує єдині стандарти ідентифікації, обміну даними або електронної взаємодії. Такий підхід призводить до множинності платформ, дублювання функцій та нерівномірності цифрового розвитку державних інституцій.

4. Дефіцит кваліфікованих кадрів і цифрових компетентностей – обмежує спроможність органів державної влади самостійно впроваджувати, адмініструвати та розвивати цифрові технології. Конкретним прикладом є ситуація, коли державна установа впроваджує складну інформаційну систему, але не має достатньої кількості фахівців із кібербезпеки, аналізу даних, системної інтеграції чи управління цифровими проєктами. Це підвищує залежність від зовнішніх підрядників та створює ризики неналежного супроводу систем після завершення проєкту.

5. Недостатня узгодженість управлінських процесів – характеризується невідповідністю цифрових інструментів реальним адміністративним процедурам та організаційній структурі державної інституції. Показовим прикладом є автоматизація процедури, яка сама по собі містить надмірну кількість погоджень, дублювання функцій або зайвих етапів контролю. У такому випадку цифровізація не усуває неефективність процесу, а лише переносить її в електронне середовище, що може призводити до автоматизованого відтворення нераціональних управлінських практик.

6. Ризик неефективного використання фінансових і людських ресурсів – виникає за недостатньо обґрунтованого планування цифрових проєктів, дублювання інвестицій, необґрунтованого вибору технологічних рішень або нераціонального розподілу кадрового потенціалу. Прикладом може бути одночасне фінансування декількох цифрових платформ із подібним функціоналом різними органами влади або придбання програмного забезпечення, можливості якого не відповідають реальним потребам установи. Додатковим проявом є концентрація значних кадрових ресурсів на підтримці окремих цифрових систем замість їх спрямування на стратегічні напрями цифрової трансформації.

Таким чином, конкретні прояви організаційних ризиків демонструють, що проблеми цифровізації державного управління виникають не лише на рівні технологічного забезпечення, а значною мірою зумовлюються якістю інституційної організації, координації, кадрового забезпечення та управління ресурсами. Відповідно, мінімізація таких ризиків потребує переходу від фрагментарного впровадження окремих цифрових рішень до системного управління цифровою трансформацією, заснованого на інституційній координації, процесному підході, розвитку цифрових компетентностей та стратегічному розподілі ресурсів.

Водночас організаційна спроможність публічних інституцій не забезпечує результативності цифрової трансформації без належного технологічного забезпечення, яке визначає можливості інтеграції інформаційних систем, обміну даними, масштабування цифрових сервісів та безперервності управлінських процесів. У цьому контексті технологічні ризики пов'язані з технічними та інфраструктурними обмеженнями, які можуть знижувати ефективність цифрових інновацій, ускладнювати міжвідомчу взаємодію та створювати передумови для порушення стабільності функціонування публічних інституцій (табл. 1).

Наведена систематизація засвідчує, що технологічні ризики цифрової трансформації є взаємопов'язаними та безпосередньо впливають на спроможність публічних інституцій забезпечувати стабільність управлінських процесів і якість цифрових публічних послуг. Зокрема, несумісність інформаційних систем та недостатня інтероперабельність

Таблиця 1

Основні технологічні ризики впровадження цифрових інновацій у державному управлінні

Технологічний ризик	Основні прояви	Можливі наслідки
Несумісність інформаційних систем	Використання різних програмних платформ, форматів даних, протоколів обміну та технічних стандартів	Ускладнення автоматизованого обміну даними, дублювання інформації, збільшення кількості помилок та потреби в ручній обробці
Технологічна залежність від постачальників	Використання закритих програмних рішень, proprietary-технологій та систем, заміна яких потребує значних ресурсів	Формування vendor lock-in, зростання витрат на супровід, обмеження технологічної автономності та залежність від умов постачальника
Застарілість цифрової інфраструктури	Використання фізично та морально застарілого обладнання, програмного забезпечення та legacy-систем	Зниження надійності та продуктивності інформаційних систем, ускладнення модернізації та підвищення ймовірності технічних збоїв
Недостатня інтегрованість державних реєстрів	Дублювання інформації, відмінності у форматах даних, відсутність належної синхронізації та автоматизованого обміну	Фрагментація інформаційного середовища, повторне подання даних та зниження оперативності адміністративних процедур
Недостатня масштабованість цифрових платформ	Нездатність цифрових систем стабільно функціонувати за значного збільшення кількості користувачів, транзакцій або обсягів даних	Зниження продуктивності, перевантаження систем та тимчасова недоступність цифрових публічних послуг
Низька якість даних	Неповнота, неточність, дублювання, несвоєчасне оновлення або структурна неузгодженість даних	Зниження достовірності управлінської аналітики та ризик прийняття необґрунтованих управлінських рішень
Недостатня технологічна інтероперабельність	Відсутність узгоджених стандартів, програмних інтерфейсів та механізмів структурної й семантичної сумісності	Обмеження міжвідомчого обміну даними, ізольованість інформаційних систем та ускладнення формування єдиного цифрового середовища

Джерело: сформовано автором на основі даних [3–5]

ускладнюють інтеграцію державних реєстрів, застарілість цифрової інфраструктури обмежує можливості її модернізації, а технологічна залежність від постачальників може знижувати рівень технологічної автономності держави. Водночас низька якість даних безпосередньо впливає на достовірність управлінських рішень, тоді як недостатня масштабованість цифрових платформ створює ризики порушення доступності публічних послуг. Отже, мінімізація технологічних ризиків потребує формування інтегрованої, інтероперабельної, масштабованої та технологічно стійкої цифрової інфраструктури, яка має розглядатися як одна з базових передумов ефективного та безпечного впровадження цифрових інновацій у державному управлінні.

Враховуючи зазначене, логічним продовженням аналізу технологічних ризиків є розгляд кібербезпекових ризиків, оскільки технологічна взаємопов'язаність державних інформаційних систем одночасно розширює потенційний масштаб кіберзагроз. У цьому контексті доцільно акцентувати увагу не лише на факті кібератак, а й на їхньому потенційному впливі на безперервність державного управління, захист даних та функціонування критичної цифрової інфраструктури [6].

Зростання масштабів цифровізації державного управління супроводжується збільшенням кількості інформаційних ресурсів, цифрових сервісів, реєстрів та каналів обміну даними, що розширює поверхню потенційних кіберзагроз. Особливої небезпеки набувають кібератаки на державні інформаційні ресурси, оскільки їх наслідки можуть виходити за межі окремої інформаційної системи та впливати на функціонування цілих секторів державного управління. В Україні ця проблема має додатковий вимір через використання кіберпростору як складової гібридної агресії, спрямованої не лише на отримання інформації, а й на порушення роботи державних інституцій та критично важливих цифрових систем.

Враховуючи зазначене, доцільно навести конкретний прикладом такого ризику, адже ним може бути кібератака на державний реєстр: якщо зловмисники отримують можливість не лише викрасти інформацію, а й змінити записи, наслідком стає вже не просто

Таблиця 2

Систематизація кібербезпекових ризиків цифрової трансформації державного управління

Кібербезпековий ризик	Конкретні прояви	Потенційні наслідки	Основні заходи мінімізації
Кібератаки на державні інформаційні ресурси	DDoS-атаки, фішинг, шкідливе програмне забезпечення, ransomware, атаки на вебресурси та державні інформаційні системи	блокування або порушення роботи державних сервісів, втрата доступу до інформаційних ресурсів, зупинення окремих управлінських процесів	постійний моніторинг кіберзагроз, SOC/CERT-підрозділи, багаторівневий захист, сегментація мереж, регулярне тестування
Витік та несанкціоноване використання даних	компрометація облікових записів, викрадення баз даних, незаконне копіювання або передавання інформації	розголошення персональних і службових даних, репутаційні та правові наслідки, використання інформації у ворожих цілях	шифрування даних, багатофакторна автентифікація, розмежування доступу, аудит дій користувачів, DLP-системи
Порушення конфіденційності інформації	несанкціонований доступ до персональних, службових або стратегічно важливих даних	розкриття інформації з обмеженим доступом, порушення прав громадян, компрометація державних процесів	принцип найменших привілеїв, криптографічний захист, контроль доступу, регулярний аудит безпеки
Порушення цілісності інформації	несанкціонована модифікація записів у реєстрах, підміна даних, втручання у програмний код	прийняття помилкових управлінських рішень, спотворення державних реєстрів, юридично значущі помилки	контроль цілісності, електронний підпис, резервні копії, журналювання змін, механізми верифікації даних
Порушення доступності інформації та цифрових сервісів	DDoS, ransomware, відмова серверів, пошкодження інфраструктури	недоступність адміністративних послуг, порушення безперервності державного управління	резервування систем, географічно розподілена інфраструктура, disaster recovery, резервне копіювання
Дестабілізація критичної цифрової інфраструктури	комплексні атаки на центри обробки даних, телекомунікаційні мережі, енергетичні та інші взаємозалежні цифрові системи	системні перебої у функціонуванні держави, каскадне поширення збоїв між секторами, зниження стійкості державних інституцій	захист критичної інфраструктури, резервні контури управління, кібернавчання, міжвідомчий обмін інформацією про загрози, кризове реагування

Джерело: сформовано автором на основі даних [7–10]

витік даних, а порушення їх цілісності та достовірності. Наприклад, несанкціонована зміна відомостей у реєстрах може унеможливити отримання адміністративних послуг, створити юридичні колізії або зумовити прийняття державним органом помилкового рішення. Іншим прикладом є DDoS-атака на державний вебпортал, яка здатна тимчасово зробити недоступними електронні послуги для значної кількості громадян. Найбільш небезпечним є сценарій, за якого компрометація одного інформаційного ресурсу створює можливість проникнення до пов'язаних систем і поширення атаки на інші державні інформаційні ресурси [11].

Окрему загрозу становлять атаки типу ransomware, за яких зловмисники блокують доступ до інформаційних ресурсів шляхом шифрування даних. Для державного сектору такий сценарій є особливо критичним, оскільки навіть за умови відсутності остаточної втрати інформації тимчасова недоступність реєстру або інформаційної системи може порушити виконання державних функцій. Відповідно, кібербезпека державного управління має бути орієнтована не лише на запобігання проникненню, а й на забезпечення кіберстійкості, тобто здатності системи продовжувати функціонування, своєчасно реагувати на інциденти та відновлюватися після кібератаки.

З огляду на системний характер зазначених загроз, їх мінімізація потребує не окремих технічних рішень, а комплексної державної політики кіберстійкості. Її доцільно реалізовувати за такими напрямами [12]:

1. Посилення централізованого моніторингу кіберзагроз. Необхідним є постійний моніторинг державних інформаційних ресурсів, раннє виявлення аномальної активності та оперативний обмін інформацією про кіберінциденти між уповноваженими державними структурами.

2. Застосування багаторівневого захисту. Захист державних систем має базуватися на поєднанні багатофакторної автентифікації,

шифрування, сегментації мереж, контролю доступу, захисту кінцевих пристроїв та постійного оновлення програмного забезпечення.

3. Забезпечення резервування та відновлюваності. Критично важливі дані й системи повинні мати захищені резервні копії, альтернативні канали функціонування та заздалегідь визначені процедури відновлення після кіберінцидентів.

4. Захист державних реєстрів і критичної цифрової інфраструктури. Необхідно посилювати контроль доступу до реєстрів, здійснювати регулярний аудит їх захищеності, тестування на проникнення та сегментацію критичних компонентів, щоб компрометація одного ресурсу не призводила до каскадного поширення атаки.

5. Управління доступом і даними. Доцільно реалізовувати принцип найменших привілеїв, відповідно до якого працівник отримує лише той обсяг доступу, який необхідний для виконання службових функцій. Важливим є також журналювання операцій із даними та регулярний перегляд прав доступу.

6. Підвищення кіберкомпетентності персоналу. Значна частина кіберінцидентів пов'язана з людським фактором, тому державні установи мають регулярно проводити навчання щодо фішингу, соціальної інженерії, безпечної роботи з даними та реагування на підозрілі інциденти.

7. Регулярне тестування кіберстійкості. Державні інформаційні системи мають проходити періодичні оцінювання вразливостей, penetration testing, моделювання кіберінцидентів та навчання з відновлення роботи після масштабних атак.

8. Формування міжвідомчої системи реагування. Кіберінцидент у державному секторі не повинен розглядатися як проблема окремої установи. Необхідна узгоджена взаємодія органів державної влади, операторів критичної інфраструктури та спеціалізованих суб'єктів кібербезпеки.

У такий спосіб, кібербезпекові ризики є найбільш критичною складовою ризиків цифрової трансформації, оскільки їх реалізація може одночасно порушувати конфіденційність, цілісність і доступність інформації та створювати загрозу безперервності державного управління. При цьому кібератака на окрему інформаційну систему потенційно здатна трансформуватися у системну кризу за умови високої взаємозалежності державних цифрових ресурсів. Тому державна політика у сфері цифровізації має передбачати security-by-design, тобто інтеграцію вимог кібербезпеки на етапі проєктування цифрових систем, а не їх додавання після впровадження. Поєднання превентивного захисту, постійного моніторингу, резервування, оперативного реагування та відновлення дозволяє перейти від моделі реагування на окремі кіберінциденти до системного управління кібербезпековими ризиками та забезпечення кіберстійкості державного управління [13].

Отож, взаємопов'язаність організаційних, технологічних і кібербезпекових ризиків зумовлює необхідність формування комплексного механізму їх управління, інтегрованого у систему стратегічного управління цифровою трансформацією державного управління. Його доцільність визначається тим, що локальне реагування на окремі ризики не забезпечує належного рівня цифрової стійкості, оскільки реалізація одного ризику може посилювати інші та спричиняти кумулятивний негативний ефект.

Ключовими складовими такого механізму мають бути [14]:

– стратегічне планування цифрової трансформації – узгодження цифрових проєктів із пріоритетами та архітектурою державного управління;

– інституційна координація – забезпечення міжвідомчої взаємодії, розподілу відповідальності та узгодженості цифрових рішень;

– розвиток цифрових компетентностей – формування кадрової спроможності щодо використання технологій, управління даними та кібербезпеки;

– технологічна модернізація та інтероперабельність – оновлення цифрової інфраструктури, стандартизація та забезпечення інтегрованої взаємодії інформаційних систем;

– захист даних і кібербезпека – забезпечення конфіденційності, цілісності та доступності інформації, а також стійкості критичної цифрової інфраструктури;

– безперервний моніторинг ризиків – своєчасна ідентифікація загроз, оцінювання вразливостей, реагування та відновлення після інцидентів.

Таким чином, комплексний механізм має забезпечувати перехід від реактивного реагування на реалізовані загрози до превентивного та адаптивного управління ризиками за циклом «ідентифікація – оцінювання – мінімізація – моніторинг – реагування – відновлення». Його функціонування створює передумови для одночасного підвищення ефективності цифрової трансформації, інституційної спроможності, технологічної стійкості та кібербезпеки державного управління.

Разом з тим, ефективність цифрових інновацій у державному управлінні визначається не стільки масштабом технологічного впровадження, скільки спроможністю держави забезпечити їх системну інтеграцію в управлінські

процеси. Така інтеграція має ґрунтуватися на поєднанні технологічної надійності, кібербезпеки, інституційної узгодженості, кадрової спроможності та орієнтації на суспільні потреби. Відповідно, цифрові інновації мають розглядатися не як самоціль, а як інструмент підвищення результативності державного управління, якості публічних послуг і довіри суспільства до державних інституцій [15].

У цьому контексті результативність цифрової трансформації доцільно оцінювати за комплексом взаємопов'язаних критеріїв: ефективністю управлінських процесів, доступністю та якістю публічних послуг, технологічною стійкістю, рівнем кібербезпеки, інституційною узгодженістю та відповідністю цифрових рішень суспільним потребам. Саме така система критеріїв дає змогу перейти від оцінювання цифровізації за кількістю впроваджених технологій до визначення її реального управлінського та суспільного ефекту. Значить, ефективна цифрова трансформація державного управління потребує системного, ризик-орієнтованого та людиноцентричного підходу, за якого технологічні інновації поєднуються з інституційною спроможністю, кіберстійкістю та орієнтацією на створення публічної цінності. Це забезпечує не лише технологічне оновлення державного управління, а й формування стійкої цифрової системи, здатної адаптуватися до нових технологічних, організаційних і безпекових ризиків.

Висновки. Таким чином, упровадження цифрових інновацій у державному управлінні підвищує результативність управлінських процесів, доступність і якість публічних послуг, однак одночасно формує взаємопов'язану систему організаційних, технологічних і кібербезпекових ризиків. Обґрунтовано, що їх кумулятивний вплив може знижувати інституційну спроможність держави, порушувати безперервність управлінських процесів та дестабілізувати цифрову інфраструктуру. Визначено, що мінімізація таких ризиків потребує комплексного ризик-орієнтованого механізму, який поєднує стратегічне планування, інституційну координацію, розвиток цифрових компетентностей, технологічну модернізацію, інтероперабельність, захист даних, кібербезпеку та безперервний моніторинг ризиків. Доведено, що ефективність цифрових інновацій доцільно оцінювати не за масштабом технологічного впровадження, а за сукупністю критеріїв організаційної ефективності, технологічної стійкості, кібербезпеки, інституційної узгодженості, якості публічних послуг і суспільної результативності. Отже, цифрова трансформація державного управління має розглядатися як системний процес, результативність якого визначається здатністю держави забезпечити безпечну, стійку, інституційно узгоджену та суспільно орієнтовану інтеграцію цифрових інновацій.

Бібліографічний список

1. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління,* 2018. № 1. С. 5–10. URL: http://nbuv.gov.ua/UJRN/vnaddy_2018_1_3
2. Костенюк Н., Макарова І., Пігарєв Ю. & Сметаніна Л. Цифровізація публічного управління: вітчизняний досвід. *Теоретичні та прикладні питання державотворення,* 2021. №26. С. 41–50. DOI: https://doi.org/10.35432/tisb262021239001
3. Скляр І. Особливості розвитку цифрового врядування в умовах воєнного стану. *Аспекти публічного управління,* 2024. №12(4), С. 59–66. DOI: https://doi.org/10.15421/152449
4. Богач Ю. Цифровізація діяльності органів місцевого самоврядування як інструмент забезпечення сталого розвитку територіальних громад. *Економічний простір.* 2025. № 201. С. 264–268. URL: https://doi.org/10.30838/ep.201.264-268
5. Заболотенко Д., Герасимюк К. Цифрова трансформація місцевого самоврядування та розвиток професійних компетентностей посадових осіб місцевого самоврядування. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування».* 2024. № 1. С. 71–78. URL: https://doi.org/10.32782/2786-5681-2024-1.09
6. Цифрова адженда України-2020 («Цифровий порядок денний» – 2020). Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf
7. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник Повітряне і космічне право. НАУ.* 2021. № 2(59). С. 110–115. DOI: https://doi.org/10.18372/2307-9061.59.15603
8. Шолойко А. Кібербезпека як нова Ціль Сталого Розвитку. *Digital Economy.* 2023. Issue III (91). С. 43–52. DOI: http://doi.org/10.34025/2310-8185-2023-3.91.03
9. 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: Розпорядж.

Каб. Міністрів України від 04.06.2025 № 546-р. URL: https://zakon.rada.gov.ua/laws/show/546-2025-р#Text
10. Сіденко В. Виклики і ризики цифрової трансформації: світовий та український контексти. *Економіка України,* 2021. №64(5 (714). 40–58. https://doi.org/10.15407/economyukr.2021.05.040
11. Горбаченко С. Кібербезпека як складова економічної безпеки України. *Galician economik journal*. 2020. № 5 (66). С. 180–186. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2020.0
12. Цифровий вектор інтеграції України в ЄС: воєнні виклики сьогодення / Л. Г.Мельник та ін. *Наукові праці Міжрегіональної академії управління персоналом. Економічні науки,* 2023. № 3 (70). С. 18–26. DOI: https://doi.org/10.32689/2523-4536/70-3
13. Башлай С., Яремко І. Цифровізація економіки України в умовах євроінтеграційних процесів. *Економіка та суспільство*, 2023. № 48. DOI: https://doi.org/10.32782/2524-0072/2023-48-48
14. Іртищева І. О., Сєнкевич О. Ф. Цифрова трансформація регіонів України: об'єктивна необхідність, принципи цифрового розвитку та особливості регулювання. *Регіональна економіка,* 2020. № 1. С. 14–21. DOI: https://doi.org/10.36818/1562-0905-2020-1-2
15. Лялюк О. Ю., Степанюк К. І. Проблеми правового регулювання електронного урядування в діяльності органів місцевого самоврядування. *Юридичний науковий електронний журнал,* 2024. № 3. С. 82–86. URL: https://doi.org/10.32782/2524-0374/2024-3/17

References

1. Kuibida V. S., Karpenko O. V., Namestnik V. V. (2018) Tsyfrove vriaduvannia v Ukraini: bazovi definitsii poniatiino-katehorialnoho aparatu [Digital governance in Ukraine: basic definitions of the conceptual and categorical framework]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy. Seriia: Derzhavne upravlinnia*, no. 1, pp. 5–10. Available at: http://nbuv.gov.ua/UJRN/vnaddy_2018_1_3 (in Ukrainian)
2. Kosteniuk N., Makarova I., Pihariev Yu., Smetanina L. (2021) Tsyfrovizatsiia publichnoho upravlinnia: vitchyznianyi dosvid [Digitalization of public administration: domestic experience]. *Teoretychni ta prykladni pytannia derzhavotvorennia,* no. 26, pp. 41–50. DOI: https://doi.org/10.35432/tisb262021239001 (in Ukrainian)
3. Skliar I. (2024) Osoblyvosti rozvytku tsyfrovoho vriaduvannia v umovakh voiennoho stanu [Features of digital governance development under martial law]. *Aspekty publichnoho upravlinnia,* vol. 12, no. 4, pp. 59–66. DOI: https://doi.org/10.15421/152449 (in Ukrainian)
4. Bohach Yu. (2025) Tsyfrovizatsiia diialnosti orhaniv mistsevoho samovriaduvannia yak instrument zabezpechennia staloho rozvytku terytorialnykh hromad [Digitalization of local government bodies' activities as a tool for ensuring sustainable development of territorial communities]. *Ekonomichnyi prostir,* no. 201, pp. 264–268. DOI: https://doi.org/10.30838/ep.201.264-268 (in Ukrainian)
5. Zabolotenko D., Herasymiuk K. (2024) Tsyfrova transformatsiia mistsevoho samovriaduvannia ta rozvytok profesiinykh kompetentnostei posadovykh osib mistsevoho samovriaduvannia [Digital transformation of local self-government and development of professional competencies of local government officials]. *Naukovyi visnyk Vinnytskoi akademii bezperervnoi osvity. Seriia "Ekolohiia. Publichne upravlinnia ta administruvannia",* no. 1, pp. 71–78. DOI: https://doi.org/10.32782/2786-5681-2024-1.09 (in Ukrainian)
6. Tsyfrova adzhenda Ukrainy-2020 ("Tsyfrovyi poriadok dennyi" – 2020). Kontseptualni zasady (versiia 1.0). Pershocherhovi sfery, initsiatyvy, proekty "tsyfrovizatsii" Ukrainy do 2020 roku [Digital Agenda of Ukraine-2020 ("Digital Agenda" – 2020). Conceptual framework (version 1.0). Priority areas, initiatives and digitalization projects of Ukraine until 2020]. Available at: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (in Ukrainian)
7. Sopilko I. M. (2021) Informatsiina bezpeka ta kiberbezpeka: porivnialno-pravovyi aspekt [Information security and cybersecurity: comparative legal aspect]. *Yurydychnyi visnyk. Povitriane i kosmichne pravo*, no. 2 (59), pp. 110–115. DOI: https://doi.org/10.18372/2307-9061.59.15603 (in Ukrainian)
8. Sholoiko A. (2023) Kiberbezpeka yak nova Tsil Staloho Rozvytku [Cybersecurity as a new Sustainable Development Goal]. *Digital Economy,* issue III (91), pp. 43–52. DOI: https://doi.org/10.34025/2310-8185-2023-3.91.03 (in Ukrainian)
9. Pro skhvalennia Stratehii rozvytku sfery elektronnykh komunikatsii Ukrainy na period do 2030 roku ta zatverdzhennia operatsiinoho planu zakhodiv z yii realizatsii u 2025–2027 rokakh (2025) [On approval of the Strategy for the development of electronic communications in Ukraine for the period until 2030 and approval of the operational action plan for its implementation in 2025–2027]. Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 04.06.2025 № 546-r. Available at: https://zakon.rada.gov.ua/laws/show/546-2025-p#Text (in Ukrainian)
10. Sidenko V. (2021) Vyklyky i ryzyky tsyfrovoi transformatsii: svitovyi ta ukrainskyi konteksty [Challenges and risks of digital transformation: global and Ukrainian contexts]. *Ekonomika Ukrainy,* vol. 64 (714), no. 5, pp. 40–58. DOI: https://doi.org/10.15407/economyukr.2021.05.040 (in Ukrainian)
11. Horbachenko S. (2020) Kiberbezpeka yak skladova ekonomichnoi bezpeky Ukrainy [Cybersecurity as a component of Ukraine's economic security]. *Halytskyi ekonomichnyi visnyk,* no. 5 (66), pp. 180–186. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2020.0 (in Ukrainian)

12. Melnyk L. H. et al. (2023) Tsyfrovyi vektor intehratsii Ukrainy v YeS: voienni vyklyky sohodennia [Digital vector of Ukraine's integration into the EU: current wartime challenges]. *Naukovi pratsi Mizhnarodnoi akademii upravlinnia personalom. Ekonomichni nauky,* no. 3 (70), pp. 18–26. DOI: https://doi.org/10.32689/2523-4536/70-3 (in Ukrainian)
13. Bashlai S., Yaremko I. (2023) Tsyfrovizatsiia ekonomiky Ukrainy v umovakh yevrointehratsiinykh protsesiv [Digitalization of Ukraine's economy in the context of European integration processes]. *Ekonomika ta suspilstvo,* no. 48. DOI: https://doi.org/10.32782/2524-0072/2023-48-48 (in Ukrainian)
14. Irtyshcheva I. O., Sienkevych O. F. (2020) Tsyfrova transformatsiia rehioniv Ukrainy: obiektyvna neobkhidnist, pryntsypy tsyfrovoho rozvytku ta osoblyvosti rehuliuvannia [Digital transformation of the regions of Ukraine: objective necessity, principles of digital development and regulatory features]. *Rehionalna ekonomika,* no. 1, pp. 14–21. DOI: https://doi.org/10.36818/1562-0905-2020-1-2 (in Ukrainian)
15. Lialiuk O. Yu., Stepaniuk K. I. (2024) Problemy pravovoho rehuliuvannia elektronnoho uriaduvannia v diialnosti orhaniv mistsevoho samovriaduvannia [Problems of legal regulation of e-government in the activities of local self-government bodies]. *Yurydychnyi naukovyi elektronnyi zhurnal,* no. 3, pp. 82–86. DOI: https://doi.org/10.32782/2524-0374/2024-3/17 (in Ukrainian)

Anna Kyrychenko
PhD in Public Administration,
Head of the Department of Postgraduate and Doctoral Studies,
Higher Educational Institution "Open International University
of Human Development "Ukraine"
ORCID: https://orcid.org/0000-0003-1067-8758

RISKS AND CHALLENGES OF IMPLEMENTING DIGITAL INNOVATIONS IN PUBLIC ADMINISTRATION: ORGANIZATIONAL, TECHNOLOGICAL AND CYBERSECURITY ASPECTS

This article examines the risks and challenges that arise during the implementation of digital innovations in the public administration system, taking into account the organizational, technological, and cybersecurity aspects of digital transformation. It is argued that the digitization of public administration, while improving the efficiency of management processes, the accessibility of public services, transparency, and the speed of decision-making, also creates new sources of systemic risks capable of affecting the stability and continuity of public institutions' operations. The main organizational risks of digital innovation have been systematized, including institutional resistance to change, insufficient coordination among government agencies, the fragmented nature of digital transformations, a shortage of qualified personnel, insufficient alignment of management processes, and risks associated with the inefficient use of financial and human resources. Particular attention was paid to cybersecurity risks, specifically the increasing number of cyberattacks on government information resources, threats of data leaks and unauthorized use, breaches of confidentiality, integrity, and availability of information, as well as risks of destabilization of critical digital infrastructure. It is proposed that the risks of digital innovations be considered as an interconnected system in which organizational, technological, and cybersecurity factors mutually reinforce one another. The paper justifies the need for a comprehensive mechanism to manage such risks, which should combine strategic planning for digital transformation, institutional coordination, the development of digital competencies, technological modernization, standardization and interoperability of information systems, data protection, cybersecurity, and continuous risk monitoring. It has been determined that the effectiveness of digital innovations in public administration depends on the state's ability not only to implement new technologies but also to ensure their secure, sustainable, institutionally coordinated, and socially oriented integration into the public administration system.

Keywords: digital transformation, risks, digital innovation, public administration, cybersecurity, innovation, risk management, digital governance.

Дата надходження статті: 17.09.2026
Дата прийняття статті до публікації: 21.10.2026
Дата публікації статті: 18.11.2026