

ПУБЛІЧНЕ УПРАВЛІННЯ РОЗВИТКОМ ІНФРАСТРУКТУРИ ЦИФРОВОГО УРЯДУВАННЯ: СТРАТЕГІЧНІ ПРІОРИТЕТИ ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ СИСТЕМНОЇ СТІЙКОСТІ

О. О. Вітюк, к. і. н., старший викладач, Вінницький державний педагогічний університет імені Михайла Коцюбинського, voo_32@ukr.net, orcid.org/0009-0007-1749-507X

Методологія дослідження. В основу дослідження покладено гармонійне поєднання загальнонаукових і спеціальних методів, що забезпечило об'єктивність, цілісність та достовірність сформульованих висновків. Вибір методологічної бази визначено специфікою цифрового урядування як складної соціотехнічної системи, вивчення якої потребує міждисциплінарного синтезу публічного адміністрування, інформаційного права та кібербезпеки. Завдяки системно-структурному та системно-функціональному аналізу інфраструктуру цифрового урядування концептуалізовано як цілісний об'єкт публічного управління. Застосування цих методів дозволило декомпонувати зазначену інфраструктуру на взаємопов'язані рівні та розкрити функціональну взаємодію між ними. Метод інституційного аналізу застосовано для дослідження нормативно-правового та організаційного забезпечення цифрової трансформації, зокрема розподілу повноважень між суб'єктами публічного управління, функціонування інституту CDTO.

Результати. Встановлено, що цифрове урядування сьогодні потребує балансу між відкритістю сервісів та безпекою даних. Його системна стійкість полягає у здатності державних платформ адаптуватися до загроз, працювати безперебійно та швидко відновлюватися після кризових ситуацій. Обґрунтовано стратегічні пріоритети державного регулювання цифрової інфраструктури, серед яких ключове значення мають забезпечення повної інтероперабельності даних за принципом *Once Only*, перехід на хмарні технології, дотримання підходу *Digital by Design*, а також гарантування безбар'єрності та доступності цифрових послуг. Гармонізація цих пріоритетів із міжнародними стандартами є обов'язковою умовою інтеграції національного цифрового простору до глобального середовища.

Новизна. Структуровано інфраструктуру цифрового урядування як об'єкта публічно-управлінського впливу, шляхом виокремлення та систематизації взаємопов'язаних рівнів, що дозволяє здійснювати точкове та системне регулювання цифрових трансформацій.

Практична значущість. Сформульовано концептуальні засади забезпечення системної стійкості інфраструктури цифрового урядування як динамічної спроможності публічно-управлінської системи адаптуватися до деструктивних впливів, зберігати безперервність надання державних послуг та відновлювати функціональність шляхом поетапного поєднання технологічно-кібербезпекового, функціонально-процесуального та інституційно-кадрового вимірів. Обґрунтовано модель оптимізації публічного управління цифровою інфраструктурою в умовах кризових станів, яка базується на поєднанні децентралізованої міжвідомчої взаємодії, превентивної релокації баз даних у закордонні хмарні сховища та оперативності антикризових платформових рішень. Консолідація державних реєстрів та інституційне посилення кіберзахисту на рівні органів місцевого самоврядування потребуватиме подальшого підсилення як інструменту підвищення адаптивності цифрових систем.

Ключові слова: публічне управління, цифрове урядування, інфраструктура цифрового урядування, системна стійкість, цифрова трансформація, інтероперабельність, державні реєстри, кібербезпека, хмарні технології.

Постановка проблеми. Динамічний розвиток зручних електронних послуг випередив готовність самої цифрової інфраструктури держави, таким чином виявивши проблеми з безпекою та стійкістю. Непослідовна нормативна база, технічний розрив між центром і громадами, дефіцит фахівців та ризики витоку даних створюють загрози для публічного управління. Розв'язати це можна лише через докорінну зміну механізмів державного регулювання та фокус на побудові захищеної інфраструктури.

Залежність державних структур від цифрових платформ і реєстрів виявилась у нових викликах. Спостерігається суперечність між високим ступенем централізації й взаємопов'язаності державних інформаційних ресурсів та уразливістю їхньої фізичної і мережевої інфраструктури. Виникає гостра потреба у масштабному переході на хмарні та розподілені технології. На сьогодні існує неузгодженість між наявними нормативно-правовими механізмами публічного управління та реальною динамікою цифрових загроз. Більшість законодавчих вимог орієнтовані на «статичну» безпеку та дотримання формальних процедур захисту інформації, тоді як сучасні умови вимагають застосування динамічної системної стійкості.

Слід констатувати, що маємо наявну суттєву диспропорцію в рівнях захищеності та технологічного оснащення між центральними органами виконавчої влади та органами місцевого самоврядування. При потужних цифрових екосистемах та залучених висококваліфікованих кадрів на центральному рівні, на рівні громад цифрова інфраструктура нерідко залишається найбільш уразливою для масштабних кібератак та порушень цілісності державних реєстрів.

Аналіз останніх досліджень і публікацій. Питання розвитку цифрового урядування та забезпечення інституційної стійкості публічного сектору є предметом активного наукового дискурсу в нашій державі. Дослідницький вектор у цій сфері поступово змістився від аналізу первинної автоматизації державних послуг до осмислення цифровізації як комплексної соціотехнічної системи через призму забезпечення інституційної стійкості. Застосування цифрових технологій оптимізує надання публічних послуг,

забезпечуючи їх оперативність та доступність, а також дозволяє трансформувати сервіси на засадах персоніфікації й адресності з урахуванням специфічних потреб громадян і суб'єктів господарювання (Н. Корчак, А. Рачинський, Н. Ларіна) [1]. На відміну від електронного уряду, орієнтованого переважно на первинне впровадження цифрових технологій у роботу органів влади, цифрове урядування передбачає їхню глибинну інтеграцію задля досягнення синергетичного ефекту та безперервної модернізації систем державного й регіонального управління (В. Нагаєв, О. Гіржева, І. Чалий, С. Міненко) [2]. Реалізація концепції електронного урядування є багатоаспектним завданням, яке потребує суттєвих інвестиційних ресурсів і системного подолання комплексу взаємопов'язаних політико-право-вих, організаційно-адміністративних та інфраструктурних викликів (Т. Голобородько, О. Дубіна) [3].

Окрім того, відзначимо, що теоретико-методологічні засади визначення змісту, сутності та цільової спрямованості цифрових комунікацій і кібербезпеки в сфері публічного адміністрування висвітлено у працях К. Герасимюка [4], Г. Жекало, М. Заяць, О. Вакун [5], Т. Забейворота [6] та О. Мазура [7].

Нормативно-правову базу дослідження становлять Конституція України [10], Закони України «Про хмарні послуги» [8], «Про основні засади забезпечення кібербезпеки України» [9], «Про захист персональних даних» [11] та «Про особливості надання публічних (електронних публічних) послуг» [12].

Попри наявність численних розробок, управлінські засади забезпечення системної стійкості безпосередньо інфраструктури цифрового урядування досі не отримали належного комплексного висвітлення. Наявні праці здебільшого обмежені вивченням окремих технічних (кіберзахисних) аспектів або теоретичних концепцій публічного адміністрування, відірваних від технологічного підґрунтя. Практично поза увагою дослідників залишається поєднання нормативно-правових, інституційних та ресурсних механізмів управління інфраструктурними об'єктами в умовах безпекових загроз і воєнного

стану, що й обґрунтовує актуальність даного дослідження.

Формулювання мети статті. Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій щодо вдосконалення механізмів публічного управління розвитком інфраструктури цифрового урядування задля забезпечення її системної стійкості та стратегічної ефективності.

Виклад основного матеріалу дослідження. У сучасній теорії публічного управління інфраструктура цифрового урядування розглядається не просто як сукупність технічних засобів або програмного забезпечення, а як середовищно-утворювальний комплекс (соціотехнічна система), який забезпечує взаємодію між державою, бізнесом і громадянами в цифровому форматі. Як об'єкт публічно-управлінського впливу, інфраструктура цифрового урядування охоплює декілька взаємопов'язаних рівнів: нормативно-правовий та стандартизаційний рівень: закони [8], технічні регламенти та єдині стандарти інформаційного обміну; інституційно-організаційний рівень: суб'єкти публічного управління (міністерства, відомства, цифрові офіси, регулятори); базовий технологічний (апаратний) рівень: фізичні сервери, центри обробки даних (ЦОД), мережі зв'язку; платформно-прикладний рівень: державні електронні реєстри, системи інтероперабельності, сервіси цифрової ідентифікації та рівень даних: електронні бази даних та відкриті дані як ресурс прийняття рішення.

Під системною стійкістю (*systemic resilience*) інфраструктури цифрового урядування варто розуміти спроможність публічно-управлінських та технологічних компонентів адаптуватися до деструктивних чинників, забезпечувати безперервність функціонування державних платформ і мінімізувати час відновлення після кризових збоїв. У контексті публічного управління системну стійкість доцільно розглядати через три основні виміри: технологічний і кібербезпековий, функціонально-процесуальний та інституційно-кадровий. При технологічному та кібербезпековому вимірі стійкості особливого змісту набуває здатність апаратного та програмного забезпечення про-

тистояти кіберзагрозам [9]; функціонально-процесуальний – вимірюється здатністю публічних інститутів безперебійно надавати послуги; наявність правової бази, розподілу відповідальності та кваліфікованого персоналу з достатнім рівнем цифрової грамотності – основа для інституційно-кадрового виміру стійкості.

Стратегічними пріоритетами розвитку інфраструктури цифрового урядування є ключові орієнтири державного регулювання у цій сфері, які охоплюють такі напрями, зокрема, повна інтероперабельність даних та систем за принципом *Once Only* [13], принцип *Digital by Design / Digital by Default* у нормотворчій діяльності [14], хмарно-орієнтована архітектура (*Cloud-First Strategy*) на основі спеціального законодавчого регулювання [8]. Ключовими векторами у гармонізації національних стратегічних пріоритетів із міжнародними стандартами на сьогодні залишаються імплементація вимог Європейської рамки інтероперабельності (EIF) для забезпечення сумісності на правовому, організаційному, семантичному та технічному рівнях [імплементації] та дотримання стандартів кібербезпеки та захисту даних (GDPR та NIS2 Directive) [17].

Механізми забезпечення системної стійкості в публічному управлінні охоплює централізацію стратегічного керівництва при децентралізації виконання, тобто, формування єдиного координаційного центру для визначення архітектурних стандартів та технічних вимог, у поєднанні із наданням операційної автономії галузевим відомствам і органам місцевого самоврядування; інституціалізацію посади керівника цифрової трансформації (CDTO) на всіх рівнях владної вертикалі [19], запровадження інституту CDTO на всіх рівнях публічного адміністрування (у міністерствах, обласних та міських адміністраціях) забезпечить наскрізну вертикаль управління, спростить міжвідомчу комунікацію та буде гарантом дотримання єдиної цифрової політики, створення спеціалізованих центрів реагування на інциденти (CERT/CSIRT) [8], фактично це команди швидкого реагування на кіберінциденти у публічному секторі, що будуть здійснювати цілодобовий моніторинг стану безпеки, обмін інформацією про загрози та забезпечу-

ватимуть операційну координацію під час кризових ситуацій.

Важливим компонентом механізму системної стійкості залишається урегулювання його нормативно-правової бази. Нормативно-правовий механізм забезпечує легітимне підґрунтя для адаптивного функціонування інфраструктури та регламентує суб'єкту взаємодію в цифровому просторі, зокрема в умовах правових режимів надзвичайного чи воєнного стану та критичного зростання рівнів безпекових загроз. Ключовими складовими виступають: законодавче закріплення режимів безперервності діяльності (Business Continuity Plan) (нормативна обов'язковість розробки, регулярного тестування та оновлення планів безперервності діяльності для всіх суб'єктів, що утримують державні електронні реєстри та критичні інформаційні системи) [16]; правове регулювання використання хмарних технологій (Cloud Government Policy) (створення гнучкого законодавчого поля для розміщення державних даних у закордонних ЦОД або на платформах міжнародних хмарних провайдерів у разі виникнення загрози фізичного знищення вітчизняної інфраструктури); нормативна стандартизація інтероперабельності та відкритих даних (закріплення обов'язкових технічних та семантичних протоколів взаємодії, що виключає монополізацію розробки програмного забезпечення окремими підрядниками та гарантує вендор-незалежність державних систем).

Українська модель публічного управління інфраструктурою цифрового урядування продемонструвала унікальну адаптивність і життєздатність в умовах повномасштабного воєнного стану, системних кібератак та пошкоджень енергетичної та телекомунікаційної інфраструктури. Практичний досвід України став глобальним кейсом реалізації концепції системної стійкості на практиці. Завдяки застосуванню розподіленої архітектури та єдиних протоколів безпечного обміну даними на основі естонського рішення *X-Road* [18], система дала змогу уникнути створення єдиної «точки відмови». Навіть у разі збоїв у окремих відомчих базах даних загальний каркас міжвідомчої взаємодії залишався працездатним. Прийняття оперативних змін до законодавства

України про хмарні послуги дозволило внести критично важливі державні реєстри та системи (зокрема баз даних державних фінансів, демографічного реєстру тощо) до закордонних центрів обробки даних провідних світових провайдерів (AWS, Microsoft Azure, Google Cloud). Це убезпечило дані від фізичного знищення внаслідок ракетних ударів. Перетворення мобільного застосунку та порталу «Дія» на універсальний інструмент антикризового управління. Платформа зберегла доступ громадян до базових документів та соціальних виплат, а також була оперативно адаптована під нові потреби воєнного часу (фіксація пошкодженого майна, статус ВПО, подання заяв на компенсації, збір коштів на підтримку оборони).

Висновки. У науковій статті здійснено теоретичне узагальнення та запропоновано практичне розв'язання науково-прикладного завдання щодо вдосконалення механізмів публічного управління розвитком інфраструктури цифрового урядування із фокусом на забезпечення її системної стійкості. Доведено, що інфраструктура цифрового урядування в сучасній теорії публічного управління виступає не просто як сукупність технічних та інформаційних засобів, а як складна соціотехнічна система. Вона вимагає балансування між відкритістю сервісів для громадян та високим рівнем захищеності критичних баз даних. Системна стійкість визначена як динамічна спроможність публічно-управлінських та технологічних структур адаптуватися до деструктивних зовнішніх впливів, зберігати функціональність державних платформ і швидко відновлювати роботу у разі кризових ситуацій.

Обґрунтовано стратегічні пріоритети державного регулювання цифрової інфраструктури, серед яких ключове значення мають: забезпечення повної інтероперабельності даних за принципом *Once Only*, перехід на хмарні технології (*Cloud-First*), дотримання підходу *Digital by Design*, а також гарантування безбар'єрності та доступності цифрових послуг. Гармонізація цих пріоритетів із міжнародними стандартами є обов'язковою умовою інтеграції національного цифрового простору до глобального середовища. Систематизовано комплексну систему механізмів забезпечення стійкості в

публічному управлінні. На основі аналізу досвіду України показано, що успішна протидія безпековим викликам стала можливою завдяки розподіленій архітектурі системи інтегрованості, вчасній релокації баз даних у міжнародні хмари та гнучкості мобільної платформи «Дія». Для подальшої оптимізації публічного управління запропоновано посилити інституційну кіберстійкість органів місцевого самоврядування, провести дедуплікацію та консолідацію державних реєстрів на єдиній платформі, впровадити обов'язкове стрес-тестування систем і створити спеціальні мотиваційні програми для утримання ІТ-фахівців у публічному секторі.

Перспективами подальших наукових розробок у даному напрямі є дослідження оцінки економічної ефективності впровадження хмарних рішень у публічному секторі в довгостроковій перспективі.

Література

1. Корчак Н., Рачинський А., Ларіна Н. Цифрова трансформація та електронне урядування: наукові підходи дослідження в сфері публічного управління та адміністрування. *Аспекти публічного управління*. 2023. Т. 11. № 3. С. 43-49. DOI: <https://doi.org/10.15421/152334>.
2. Нагаєв В., Гіржева О., Чалий І., Міненко С. Digital трансформації публічних комунікацій, кібербезпеки та цифрового лідерства в системі електронного урядування. *Електронне наукове видання «Публічне адміністрування та національна безпека»*. 2024. № 4(45). С. 78-88. DOI: <https://doi.org/10.25313/2617-572X-2024-4-9837>.
3. Голобородько Т., Дубіна О. Використання інформаційних технологій в публічному адмініструванні: досвід України та європейські орієнтири. *Державне управління: удосконалення та розвиток*. 2018. №6. URL: <http://www.dy.nayka.com.ua/?op=1&z=1260>.
4. Герасимюк К. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. *Економіка, управління та адміністрування*. 2021. № 3(97). С. 36-40. doi: [https://doi.org/10.26642/ema-2021-3\(97\)-36-40](https://doi.org/10.26642/ema-2021-3(97)-36-40).
5. Жекало Г., Заяць М., Вакун О. Сутність та зміст електронного урядування: концептуальний вимір. *Державне управління: удосконалення та розвиток*. 2020. № 8. doi: 10.32702/2307-2156-2020.8.52.
6. Забейворота Т. Сучасна концепція е-урядування як основа модернізації системи державного управління. *Актуальні проблеми державного управління*. 2017. № 1(51). С. 35-42.
7. Мазур О. Сучасні тенденції упровадження електронного урядування в публічному управлінні:

зарубіжний досвід. *Аспекти публічного управління*. 2019. Т. 7. № 12. С. 147-156.

<https://doi.org/10.15421/151974>

8. Про хмарні послуги: Закон України від 17 лютого 2022 р. № 2075-IX. Відомості Верховної Ради України. 2023. № 15. Ст. 52.

9. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

10. Конституція України: Закон України від 28 червня 1996 р. № 254к/96–ВР. Відомості Верховної Ради. 1996. № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.

11. Про захист персональних даних: Закон України від 01 червня 2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.

12. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 р. № 1689-IX. Відомості Верховної Ради України. 2021. № 47. Ст. 383. URL: <https://zakon.rada.gov.ua/laws/show/1689-20#Text>.

13. Як Україні стати частиною цифрового простору ЄС. URL: <https://thedigital.gov.ua/news/technologies/yak-ukraini-stati-chastinoyu-tsifrovogo-prostoru-es-proveli-seminar-dlya-ministerstv>.

14. Digital by default («цифровий за замовчанням»). URL: <https://oldegap.eef.org.ua/projects/digital-by-default-tsyfrovyyi-za-zamovchanniam/>.

15. Впровадження європейських стандартів сумісності: Україна і ЄС погодили план імплементації Interoperable Europe Act. URL: <https://thedigital.gov.ua/news/technologies/vprovadzeniia-yeuropeyskykh-standartiv-sumisnosti-ukrayina-i-yes-pohodyly-plan-implementatsiyi-interoperable-europe-act>.

16. BCP (Business Continuity Plan) та DRP (Disaster Recovery Plan). Сучасні підходи до Кібербезпеки та Бізнес-Захисту. URL: https://eska.global/blog/bcp-business-continuity-plan-ta-drp-disaster-recovery-plan-suchasni-pidhodi-do-kiberbezpeki-ta-biznes-zahistu_1.

17. Від GDPR до NIS2: чому захист персональних даних більше не дорівнює кібербезпеці. URL: <https://yur-gazeta.com/dumka-eksperta/vid-gdpr-do-nis2-chomu-zahist-personalnih-danih-bilshe-ne-dorivnyue-kiberbezpeki.html>.

18. Публічний кодекс на практиці. Як проєкт X-Road став успішним міжнародним проєктом з відкритим кодом. URL: <https://ua.linkedin.com/pulse/public-code-practice-how-estonia-x-road-project-became?tl=uk>.

19. Хто такі CDTO, як вони цифровізують регіони та створюють комфортні послуги для кожного українця. URL: https://bit.ua/blog_columns/hto-taki-cdto/.

References

1. Korchak, N., Rachynskyi, A., & Larina, N. (2023). Tsyfrova transformatsiia ta elektronne

vriaduvannia: naukovi pidkhody doslidzhennia v sferi publicznego upravlinnia ta administruvannia. Aspekty publicznego upravlinnia, T.11, (3), 43-49. DOI: <https://doi.org/10.15421/152334>.

2. Nahaiev, V., Hirzheva, O., Chalyi, I., & Minenko, S. (2024). Digital transformatsii publichnykh komunikatsii, kiberbezpeky ta tsyfrovoho liderstva v systemi elektronnoho uriaduvannia. Elektronne naukovye vydannia «Publichne administruvannia ta natsionalna bezpeka», 4(45), 78-88. DOI: <https://doi.org/10.25313/2617-572X-2024-4-9837>.

3. Holoborodko, T., & Dubina, O. (2018). Vykorystannia informatsiinykh tekhnolohii v publichnomu administruvanni: dosvid Ukrainy ta yevropeiski oriientyry. Derzhavne upravlinnia: udoskonalennia ta rozvytok, (6). Retrieved from <http://www.dy.nayka.com.ua/?op=1&z=1260>.

4. Herasymuk, K. (2021). Mekhanizmy derzhavnoho upravlinnia kiber- ta informatsiinoiu bezpekoiu: problemy ta shliakhy vyrishennia. Ekonomika, upravlinnia ta administruvannia, 3(97), 36-40. doi: [https://doi.org/10.26642/ema-2021-3\(97\)-36-40](https://doi.org/10.26642/ema-2021-3(97)-36-40).

5. Zhekalo, H., Zaiats, M., & Vakun, O. (2020). Sutnist ta zmist elektronnoho uriaduvannia: kontseptualnyi vymir. Derzhavne upravlinnia: udoskonalennia ta rozvytok, (8). doi: 10.32702/2307-2156-2020.8.52.

6. Zabeivorota, T. (2017). Suchasna kontseptsiiia e-vriaduvannia yak osnova modernizatsii systemy derzhavnoho upravlinnia. Aktualni problemy derzhavnoho upravlinnia, 1(51), 35-42.

7. Mazur, O. (2019). Suchasni tendentsii uprovozhdzhennia elektronnoho uriaduvannia v publichnomu upravlinni: zarubizhnyi dosvid. Aspekty publicznego upravlinnia, T. 7, (12), 147-156. <https://doi.org/10.15421/151974>

8. Pro khmarni posluhy: Zakon Ukrainy vid 17 liutoho 2022 r. № 2075-IX. Vidomosti Verkhovnoi Rady Ukrainy (2023), № 15, St. 52.

9. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII. Vidomosti Verkhovnoi Rady Ukrainy (2017), № 45, St. 403.

10. Konstytutsiia Ukrainy: Zakon Ukrainy vid 28 chervnia 1996 r. № 254k/96–VR. Vidomosti Verkhovnoi Rady (1996), № 30, St. 141. Retrieved from

<https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.

11. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01 chervnia 2010 r. № 2297-VI. Vidomosti Verkhovnoi Rady Ukrainy (2010), № 34, St. 481. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.

12. Pro osoblyvosti nadannia publichnykh (elektronnykh publichnykh) posluh: Zakon Ukrainy vid 15 lypnia 2021 r. № 1689-IX. Vidomosti Verkhovnoi Rady Ukrainy (2021), № 47, St. 383. Retrieved from <https://zakon.rada.gov.ua/laws/show/1689-20#Text>.

13. Yak Ukraini staty chastynoiu tsyfrovoho prostoru YeS. Retrieved from <https://thedigital.gov.ua/news/technologies/yak-ukraini-stati-chastinoyu-tsifrovogo-prostoru-es-proveli-seminar-dlya-ministerstv>.

14. Digital by default («tsyfrovyyi za zamovchanniam»). Retrieved from <https://oldegap.eef.org.ua/projects/digital-by-default-tsyfrovyyi-za-zamovchanniam/>.

15. Vprovadzhenia yevropeyskykh standartiv sumisnosti: Ukraina i YeS pohodyly plan implementatsii Interoperable Europe Act. Retrieved from <https://thedigital.gov.ua/news/technologies/vprovadzhenni-a-yevropeyskykh-standartiv-sumisnosti-ukrayina-i-yes-pohodyly-plan-implementatsiyi-interoperable-europe-act>.

16. BCP (Business Continuity Plan) ta DRP (Disaster Recovery Plan). Suchasni pidkhody do Kiberbezpeky ta Biznes-Zakhystu. Retrieved from https://eska.global/blog/bcp-business-continuity-plan-ta-drp-disaster-recovery-plan-suchasni-pidhodi-do-kiberbezpeki-ta-biznes-zahistu_1.

17. Vid GDPR do NIS2: chomu zakhyst personalnykh danykh bilshe ne dorivniuye kiberbezpeksi. Retrieved from <https://yur-gazeta.com/dumka-eksperta/vid-gdpr-do-nis2-chomu-zahist-personalnih-danih-bilshe-ne-dorivnyue-kiberbezpeki.html>.

18. Publichnyi kodeks na praktytsi. Yak projekt X-Road stav uspishnym mizhnarodnym projektom z vidkrytym kodom. Retrieved from <https://ua.linkedin.com/pulse/public-code-practice-how-estonia-x-road-project-became?tl=uk>.

19. Khto taki CDTO, yak vony tsyfrovizuiut rehiony ta stvoruiut komfortni posluhy dla kozhnoho ukrainsia. Retrieved from https://bit.ua/blog_columns/hto-taki-cdto/.

PUBLIC ADMINISTRATION OF DIGITAL GOVERNANCE INFRASTRUCTURE DEVELOPMENT: STRATEGIC PRIORITIES AND MECHANISMS FOR ENSURING SYSTEMIC RESILIENCE

O. O. Vityuk, Ph. D (History), Senior Lecturer, Mykhailo Kotsiubynskyi Vinnytsia State Pedagogical University

Methods. The study is based on a harmonious combination of general scientific and specific methods, which ensured the objectivity, integrity and reliability of the formulated conclusions. The choice of methodological basis is determined by the specifics of digital governance as a complex socio-technical system, the study of which requires an interdisciplinary synthesis of public administration, information law and cybersecurity. Thanks to the system-structural and system-functional analysis, the digital governance infrastructure is conceptualized as an integral object of public administration. The application of these methods allowed to decompose the specified

infrastructure into interconnected levels and to reveal the functional interaction between them. The institutional analysis method was used to study the regulatory and organizational support of digital transformation, in particular the distribution of powers between public administration entities, the functioning of the CDTO institute.

Results. It was established that digital governance today requires a balance between the openness of services and data security. Its systemic resilience lies in the ability of state platforms to adapt to threats, operate smoothly and quickly recover from crisis situations. The strategic priorities of state regulation of digital infrastructure are substantiated, among which ensuring full data interoperability according to the Once Only principle, transition to cloud technologies, adherence to the Digital by Design approach, as well as guaranteeing barrier-free and accessible digital services are of key importance. Harmonization of these priorities with international standards is a prerequisite for the integration of the national digital space into the global environment.

Novelty. The digital governance infrastructure as an object of public administration influence is structured by isolating and systematizing interconnected levels, which allows for point and systemic regulation of digital transformations.

Practical value. There have been formulated conceptual principles for ensuring the systemic stability of the digital governance infrastructure as the dynamic ability of the public administration system to adapt to destructive influences, maintain the continuity of public services, and restore functionality through a phased combination of technological and cybersecurity, functional and procedural, and institutional and personnel dimensions. A model for optimizing public administration of digital infrastructure in times of crisis is substantiated, which is based on a combination of decentralized interagency interaction, preventive relocation of databases to foreign cloud storage and the efficiency of anti-crisis platform solutions. Consolidation of state registers and institutional strengthening of cyber protection at the level of local governments will require further strengthening as a tool for increasing the adaptability of digital systems.

Keywords: public administration, digital governance, digital governance infrastructure, system resilience, digital transformation, interoperability, state registers, cybersecurity, cloud technologies.

Стаття надійшла до редакції 23.08.2026 р.

Прийнята до публікації 08.09.2026 р.

Дата публікації 30.09.2026 р.