

<https://doi.org/10.26565/1992-2337-2026-1-11>
УДК 351: 323.2

Крутій Олена Миколаївна,
доктор наук з державного управління, професор,
професор кафедри публічної політики
навчально-наукового інституту “Інститут державного управління”
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: krutiy_elena@ukr.net <https://orcid.org/0000-0002-5180-2842>

Коротченко Наталія Олегівна,
аспірант кафедри публічної політики
навчально-наукового інституту “Інститут державного управління”
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: n.korotchenko@promodo.com <https://orcid.org/0009-0003-1365-2331>

ШЛЯХИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Анотація. У статті розглядаються основні напрямки цифрової трансформації системи державного управління в умовах гібридних загроз, що характеризуються поєднанням військових, інформаційних, кібернетичних, економічних та соціально-політичних впливів. Доведено, що цифровізація державного сектору слугує не лише інструментом модернізації адміністративних процесів, а й визначальним чинником забезпечення національної безпеки, підвищення стійкості державних інститутів та ефективності взаємодії між урядом і громадськістю. У дослідженні проаналізовано сучасні виклики цифрової трансформації, зокрема питання кібербезпеки, захисту критичної інформаційної інфраструктури, розвитку електронного урядування, цифрових послуг та механізмів електронної демократії. Визначено ключові напрями вдосконалення системи державного управління в умовах воєнного стану та під час післявоєнного відновлення України. Запропоновано комплексний комплекс практичних заходів для підвищення ефективності цифрового управління, розвитку цифрових компетентностей державних службовців та формування інтегрованої цифрової екосистеми державного управління.

Ключові слова: публічне управління, цифрова трансформація, цифровізація, гібридні загрози, кібербезпека, електронне урядування, цифрова держава, цифрові послуги, електронна демократія, національна безпека.

Як цитувати: Крутій О. М., Коротченко Н. О. Шляхи цифрової трансформації системи публічного управління в умовах гібридних загроз. *Державне будівництво*. 2026. № 1 (39). С. 157–167. <https://doi.org/10.26565/1992-2337-2025-1-11>

In cites: Krutiy, O.M., Korotchenko, N.O. (2026). Pathways of digital transformation in the public governance system amid hybrid threats. *State Formation*, no. 1 (39), 157–167. <https://doi.org/10.26565/1992-2337-2025-1-11> [in Ukrainian].

© Крутій О. М., Коротченко Н. О., 2026



This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0

Постановка проблеми. Глобальна цифровізація суспільних процесів, стрімкий розвиток інформаційно-комунікаційних технологій та зростання ролі цифрових платформ суттєво змінюють підходи до функціонування систем публічного управління. У сучасних умовах ефективність державної політики дедалі більше залежить від здатності органів влади використовувати цифрові інструменти для прийняття управлінських рішень, надання публічних послуг, взаємодії з громадянами та забезпечення належного рівня безпеки.

Особливої актуальності питання цифрової трансформації набуває в умовах гібридних загроз, які характеризуються комплексним застосуванням військових, політичних, економічних, інформаційних та кібернетичних інструментів впливу на державу. Для України проблема протидії гібридним загрозам стала однією з ключових після початку російської агресії у 2014 році та особливо загострилася після повномасштабного вторгнення у 2022 році.

Гібридні загрози суттєво трансформують вимоги до системи державного управління. Традиційні механізми реагування часто виявляються недостатньо ефективними через високу швидкість змін, масштабність ризиків та необхідність оперативного прийняття рішень. У таких умовах цифрові технології стають важливим ресурсом забезпечення стійкості держави, підтримки функціонування критичної інфраструктури, координації діяльності органів влади та комунікації з населенням.

Водночас цифрова трансформація сама по собі породжує нові ризики, пов'язані із кіберзлочинністю, кібератаками на державні інформаційні ресурси, поширенням дезінформації, маніпулятивними інформаційними кампаніями та порушенням інформаційної безпеки. Це вимагає формування нових підходів до публічного управління, які поєднують цифровізацію управлінських процесів із забезпеченням належного рівня безпеки та захисту даних.

Таким чином, дослідження шляхів цифрової трансформації системи публічного управління в умовах гібридних загроз є актуальним науковим і практичним завданням, результати якого можуть бути використані для вдосконалення державної політики цифрового розвитку та зміцнення інституційної спроможності органів влади.

Аналіз останніх досліджень і публікацій. Проблематика цифрової трансформації публічного управління перебуває у центрі уваги як зарубіжних, так і вітчизняних науковців. Теоретичні засади цифрового врядування досліджували Д. Осборн, Т. Геблер, М. Кастельс, Дж. Данліві, К. Беллами та інші. Питання розвитку електронного урядування та цифрової держави висвітлено у працях Ю. Шарова, В. Дзюндзюка, О. Крутії, І. Лопатченко, Н. Нижник, С. Домбровської, О. Дегтяр та інших учених.

Проблеми забезпечення інформаційної та кібернетичної безпеки в умовах гібридних загроз досліджували Г. Почепцов, В. Горбулін, А. Семенченко,

С. Ситник, В. Ліпкан та інші. Водночас питання комплексної цифрової трансформації системи публічного управління в умовах воєнного стану та гібридних викликів потребують подальшого наукового осмислення.

Метою роботи є дослідження основних напрямів цифрової трансформації системи публічного управління в умовах гібридних загроз та розробка рекомендацій щодо підвищення ефективності цифрового врядування в Україні.

Застосована методологія і методи. У процесі дослідження використано системний підхід, методи аналізу та синтезу, структурно-функціональний метод, порівняльний аналіз, а також метод узагальнення наукових джерел і нормативно-правових актів.

Виклад основного матеріалу. Сучасний етап розвитку системи публічного управління характеризується одночасним впливом двох взаємопов'язаних процесів: цифрової трансформації суспільства та посилення спектра гібридних загроз. Для України ця проблематика набуває особливої актуальності в умовах повномасштабної війни, коли ефективність функціонування державних інституцій безпосередньо пов'язується із забезпеченням національної безпеки, стійкості системи державного управління та здатності органів влади оперативно реагувати на кризові виклики [4; 5; 10].

Теоретичні засади цифрової трансформації державного сектору були закладені у працях зарубіжних дослідників, які обґрунтували перехід від традиційної бюрократичної моделі управління до мережевих і цифрових форм врядування. Зокрема, М. Кастельс визначив інформаційне суспільство як новий етап розвитку соціально-економічних систем, у якому ключовим ресурсом виступають знання та інформація [1]. Концепція цифрової ери врядування (Digital-Era Governance), запропонована П. Данліві та співавторами, передбачає широке використання інформаційно-комунікаційних технологій для інтеграції державних сервісів, підвищення їх доступності та орієнтації на потреби громадян [2].

У сучасних умовах цифровізація публічного управління розглядається не лише як технологічний процес, а як комплексна трансформація інституційних механізмів державного управління, що охоплює організаційні, правові, соціальні та комунікаційні аспекти діяльності органів влади [12–15]. Відповідно до міжнародних оцінок, держави, які активно впроваджують цифрові технології, демонструють вищий рівень управлінської ефективності, прозорості та стійкості до кризових впливів [4; 5; 18].

Особливістю сучасного безпекового середовища є поширення гібридних загроз, які поєднують військові, політичні, економічні, інформаційні та кібернетичні інструменти впливу. На відміну від традиційних викликів безпеки, гібридні загрози характеризуються комплексністю, прихованістю та здатністю швидко адаптуватися до змін зовнішнього середовища [10; 11]. В умовах гібридної війни особливого значення набувають питання інформа-

ційної безпеки, захисту критичної інфраструктури та забезпечення безперервності функціонування державних інституцій [8; 20].

Цифрова трансформація виступає одним із ключових інструментів підвищення стійкості системи публічного управління до зовнішніх і внутрішніх загроз. Вона забезпечує інтеграцію інформаційних ресурсів різних органів влади, автоматизацію адміністративних процедур, розвиток електронних сервісів та оперативний обмін даними між суб'єктами управління [9; 13; 14].

В Україні процес цифровізації державного сектору набув системного характеру після ухвалення низки нормативно-правових актів, спрямованих на розвиток електронного урядування та цифрової держави [7; 9]. Значну роль у цьому процесі відіграє Національна програма інформатизації, а також стратегічні документи щодо цифрового розвитку та цифрової трансформації державного управління [7; 9]. Реалізація зазначених документів сприяла формуванню сучасної цифрової інфраструктури державного сектору та створенню умов для впровадження електронних адміністративних послуг.

Одним із найбільш успішних прикладів цифрової трансформації в Україні стала екосистема електронних послуг «Дія», яка забезпечує доступ громадян до широкого спектра державних сервісів у дистанційному форматі. Особливої актуальності цифрові сервіси набули після початку повномасштабної війни, коли значна частина населення була змушена змінити місце проживання або перебувала в умовах обмеженого доступу до органів державної влади [4; 5; 9].

Використання цифрових технологій дозволило забезпечити безперервність надання адміністративних послуг, здійснювати реєстрацію внутрішньо переміщених осіб, оформлення соціальної допомоги та отримання документів незалежно від місця перебування громадян. Це стало важливим фактором підтримки соціальної стабільності та зміцнення довіри населення до державних інституцій в умовах війни [6; 9; 18].

В умовах гібридних загроз кібербезпека перетворюється на один із ключових чинників функціонування держави. Цифровізація публічного управління, з одного боку, забезпечує оперативність управлінських процесів та доступність послуг, а з іншого – збільшує вразливість державних інформаційних ресурсів до зовнішніх впливів. Кібератаки на державні органи, об'єкти критичної інфраструктури, інформаційно-комунікаційні системи та державні реєстри можуть призводити до порушення роботи органів влади, витоку персональних даних, дезорганізації суспільних процесів та зниження довіри громадян до державних інституцій [8; 20].

Повномасштабна війна проти України продемонструвала, що кіберпростір став повноцінним театром ведення бойових дій. Поряд із військовими операціями агресор систематично здійснює атаки на державні інформаційні ресурси, банківську систему, енергетичну інфраструктуру та телекомуніка-

ційні мережі. У зв'язку з цим цифрова трансформація публічного управління повинна супроводжуватися формуванням комплексної системи кіберстійкості держави, яка включатиме технічні, організаційні та нормативно-правові механізми захисту [6; 8].

Одним із перспективних напрямів є впровадження концепції кіберстійкого врядування (Cyber Resilient Governance), яка передбачає не лише захист інформаційних систем від атак, але й забезпечення їх безперервного функціонування навіть за умов часткового пошкодження або втрати окремих елементів інфраструктури. Важливими складовими такого підходу є резервування даних, використання хмарних технологій, створення географічно розподілених центрів обробки інформації та регулярне проведення аудиту кібербезпеки [18; 20].

Особливого значення набуває підготовка державних службовців до роботи в умовах кіберризиків. Низка міжнародних досліджень свідчить, що значна частина кіберінцидентів виникає через людський фактор, зокрема недостатній рівень цифрової грамотності працівників або нехтування правилами інформаційної безпеки [5; 20]. Тому формування культури кібербезпеки має стати невід'ємною складовою професійного розвитку персоналу органів державної влади.

Одним із найбільш перспективних напрямів цифрової трансформації є впровадження технологій штучного інтелекту у діяльність органів публічної влади. Сучасні системи штучного інтелекту здатні здійснювати аналіз великих обсягів інформації, прогнозувати тенденції розвитку суспільних процесів, автоматизувати рутинні адміністративні процедури та підтримувати прийняття управлінських рішень [4; 19].

У міжнародній практиці алгоритми штучного інтелекту вже використовуються для прогнозування соціально-економічних показників, аналізу ефективності державних програм, виявлення податкових правопорушень, моніторингу громадської думки та оптимізації надання адміністративних послуг [4; 5]. Для України такі технології можуть стати важливим інструментом модернізації системи публічного управління в умовах обмежених ресурсів та підвищеного навантаження на державні інституції.

Особливу роль штучний інтелект може відігравати у сфері національної безпеки та протидії гібридним загрозам. За допомогою технологій машинного навчання можливе автоматизоване виявлення дезінформаційних кампаній, аналіз інформаційних потоків у соціальних мережах, моніторинг ризиків виникнення кризових ситуацій та оцінка потенційних наслідків управлінських рішень [10; 11].

Перспективним напрямом є використання інтелектуальних чат-ботів та цифрових помічників у сфері надання адміністративних послуг. Такі рішення здатні забезпечити цілодобову підтримку громадян, автоматизувати обробку

типових запитів та скоротити навантаження на працівників державних установ [4; 16].

Водночас застосування штучного інтелекту потребує належного нормативно-правового регулювання та дотримання етичних стандартів. Особливо актуальними залишаються питання захисту персональних даних, прозорості алгоритмів прийняття рішень, недопущення дискримінації та забезпечення контролю з боку людини за діяльністю автоматизованих систем [19].

Важливим компонентом цифрового врядування є використання технологій великих даних (Big Data). Під великими даними розуміють значні масиви структурованої та неструктурованої інформації, які можуть оброблятися за допомогою сучасних аналітичних інструментів з метою виявлення закономірностей, прогнозування подій та підтримки процесу прийняття рішень [1; 16].

У публічному управлінні технології Big Data відкривають можливості для формування доказової державної політики (evidence-based policy). На відміну від традиційного підходу, що часто ґрунтується на фрагментарній статистиці або експертних оцінках, аналіз великих масивів даних дозволяє отримувати об'єктивну інформацію про реальні потреби населення та ефективність державних програм [5; 18].

Особливого значення використання великих даних набуває в умовах війни та післявоєнного відновлення. Аналіз інформації про переміщення населення, потреби внутрішньо переміщених осіб, стан критичної інфраструктури, гуманітарні потреби та рівень соціально-економічного розвитку територій дозволяє більш ефективно планувати державну політику та розподіляти ресурси [4; 18].

Використання технологій Big Data також сприяє підвищенню прозорості діяльності органів влади. Відкриті дані дозволяють громадянам, громадським організаціям та засобам масової інформації здійснювати незалежний моніторинг державних рішень, оцінювати ефективність використання бюджетних коштів та контролювати діяльність посадових осіб [5; 19].

Разом із тим впровадження аналітики великих даних потребує розвитку сучасної цифрової інфраструктури, удосконалення законодавства у сфері захисту персональних даних та підготовки фахівців, здатних працювати з великими масивами інформації.

Цифрова трансформація публічного управління неможлива без активного розвитку механізмів електронної демократії. Сучасні інформаційно-комунікаційні технології створюють нові можливості для залучення громадян до процесів формування та реалізації державної політики, сприяють підвищенню прозорості діяльності органів влади та зміцненню демократичних інститутів [2; 4].

Одним із найбільш поширених інструментів електронної демократії в Україні стали електронні петиції, громадські бюджети, електронні консультації та онлайн-платформи громадської участі. Вони дозволяють громадянам

брати участь у вирішенні питань місцевого та загальнодержавного значення незалежно від місця проживання або фізичних можливостей [9; 13].

У період воєнного стану цифрові інструменти громадської участі набули особливого значення. Вони забезпечили можливість підтримувати комунікацію між владою та громадськістю навіть в умовах вимушеного переміщення населення, обмежень безпеки та порушення транспортного сполучення. Таким чином електронна демократія стала важливим елементом забезпечення безперервності демократичних процесів в Україні [4; 9].

Розвиток електронної демократії сприяє також підвищенню рівня довіри до державних інституцій. Відкритість інформації про діяльність органів влади, можливість оперативного зворотного зв'язку та залучення громадян до ухвалення рішень формують нову модель взаємодії між державою та суспільством, яка базується на принципах партнерства та спільної відповідальності [2; 15].

Разом із тим подальший розвиток електронної демократії потребує подолання цифрової нерівності, підвищення рівня цифрової грамотності населення та забезпечення інформаційної безпеки цифрових платформ участі.

Післявоєнне відновлення України стане одним із найбільших управлінських викликів сучасності. Ефективна координація відбудови територій, залучення міжнародної допомоги, відновлення інфраструктури та забезпечення прозорості використання ресурсів вимагатимуть застосування сучасних цифрових технологій [4; 18].

Цифрові інструменти дозволяють створити єдину систему моніторингу процесів відновлення, яка забезпечуватиме збір, обробку та аналіз інформації про реалізацію проєктів відбудови. Використання цифрових платформ дає можливість громадянам відстежувати хід виконання робіт, контролювати використання бюджетних коштів та брати участь у визначенні пріоритетів розвитку територій [5; 18].

Важливим напрямом є цифровізація процесів управління міжнародною технічною допомогою. Створення інтегрованих електронних систем обліку та моніторингу міжнародних проєктів дозволить підвищити ефективність використання фінансових ресурсів, мінімізувати корупційні ризики та забезпечити прозорість процесу відбудови [4; 19].

Перспективним є також використання геоінформаційних систем, цифрових двійників територій та технологій штучного інтелекту для планування реконструкції населених пунктів, відновлення критичної інфраструктури та оцінки потреб громад. Такі технології дозволять здійснювати стратегічне планування розвитку територій на основі об'єктивних даних та прогнозних моделей.

Отже, цифрова трансформація у післявоєнний період повинна розглядатися не лише як напрям модернізації державного управління, а й як фундаментальний інструмент відновлення держави, забезпечення її конкуренто-

спроможності, зміцнення демократичних інститутів та підвищення стійкості до майбутніх безпекових викликів.

Висновки з даного дослідження та перспективи подальших досліджень. Отже, цифрова трансформація є одним із ключових напрямів модернізації системи публічного управління в умовах гібридних загроз. Її реалізація забезпечує підвищення ефективності управлінських процесів, оперативності прийняття рішень, відкритості діяльності органів влади та доступності державних послуг для населення. Водночас цифровізація виступає важливим чинником зміцнення національної стійкості та безпеки держави. Сучасні гібридні загрози вимагають переходу від традиційних адміністративних моделей до цифрових екосистем управління, здатних забезпечувати швидке реагування на кризові ситуації, інтеграцію інформаційних ресурсів та ефективну міжвідомчу взаємодію. Особливого значення набувають розвиток кібербезпеки, використання технологій штучного інтелекту, великих даних та цифрових платформ для підтримки управлінських рішень.

Важливою складовою цифрової трансформації є розвиток електронної демократії та цифрових механізмів взаємодії між державою і громадянським суспільством. Використання електронних консультацій, цифрових сервісів, онлайн-платформ участі та відкритих даних сприяє підвищенню довіри громадян до органів влади, посиленню прозорості державної політики та розширенню можливостей громадської участі у процесах управління.

Подальший розвиток цифрового публічного управління в Україні має здійснюватися на основі комплексного підходу, який поєднує технологічну модернізацію, розвиток людського капіталу, забезпечення кіберстійкості та дотримання принципів інклюзивності. У післявоєнний період цифрова трансформація повинна стати одним із стратегічних інструментів відновлення держави, забезпечення прозорості використання ресурсів та формування сучасної моделі публічного управління, орієнтованої на потреби громадян і виклики безпекового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Castells M. *The Rise of the Network Society*. 2nd ed. Oxford : Wiley-Blackwell, 2010. 597 p.
2. Dunleavy P., Margetts H., Bastow S., Tinkler J. New Public Management Is Dead – Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*. 2006. Vol. 16, No. 3. P. 467–494. <https://doi.org/10.1093/jopart/mui057>
3. Osborne D., Gaebler T. *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*. Reading, MA : Addison-Wesley Publishing Company, 1992. 405 p.
4. United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York : United Nations, 2024. 312 p. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024>

5. OECD Digital Government Index 2023: Results and Key Findings. Paris : OECD Publishing, 2023. URL: <https://www.oecd.org/gov/digital-government>
6. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI. *Відомості Верховної Ради України*. 2013. № 34–35. Ст. 458. URL: <https://zakon.rada.gov.ua/laws/show/5403-17>
7. Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20>
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
9. Стратегія цифрового розвитку, цифрових трансформацій і цифровізації державного управління України на період до 2025 року : розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р. URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-p>
10. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.
11. Почепцов Г. Г. Інформаційні війни. Київ : ВД «Києво-Могилянська академія», 2015. 497 с.
12. Семенченко А. І. Державна політика цифрового розвитку України : монографія. Київ : НАДУ, 2021. 356 с.
13. Дзюндзюк В. Б. Публічне управління та адміністрування в умовах цифровізації : монографія. Харків : Вид-во ХарPI НАДУ «Магістр», 2022. 284 с.
14. Дегтяр О. А. Цифрова трансформація публічного управління: теорія та практика : монографія. Харків : Вид-во ХарPI НАДУ, 2021. 312 с.
15. Крутій О. М. Комунікативна взаємодія в публічному управлінні : монографія. Харків : Магістр, 2020. 288 с.
16. West D. M. Digital Government: Technology and Public Sector Performance. Princeton : Princeton University Press, 2022. 352 p. <https://doi.org/10.1515/9780691228925>
17. Bellamy C., Taylor J. A. Governing in the Information Age. Buckingham : Open University Press, 1998. 240 p.
18. World Bank. GovTech Maturity Index 2024: Advancing Digital Transformation in the Public Sector. Washington, DC : The World Bank, 2024. URL: <https://www.worldbank.org/en/programs/govtech>
19. European Commission. Digital Decade Policy Programme 2030. Brussels : European Commission, 2023. URL: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
20. National Institute of Standards and Technology (NIST). Cybersecurity Framework 2.0. Gaithersburg, MD : U.S. Department of Commerce, 2024. URL: <https://www.nist.gov/cyberframework>

Стаття надійшла до редакції 25.03.2026 р.

Стаття рекомендована до друку 30.04.2026 р.

Опубліковано 30.05.2026 р.

Krutiya O. M.,

*Dr.Sc. in Public Administration, Professor,
Professor of the Department of Public Policy,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: krutiya_elenia@ukr.net <https://orcid.org/0000-0002-5180-2842>*

Korotchenko N. O.,

*Postgraduate student of the Department of Public Policy,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: n.korotchenko@promodo.com <https://orcid.org/0009-0003-1365-2331>*

PATHWAYS OF DIGITAL TRANSFORMATION IN THE PUBLIC GOVERNANCE SYSTEM AMID HYBRID THREATS

Abstract. The article examines the main directions of the digital transformation of the public governance system amid hybrid threats characterized by a combination of military, informational, cyber, economic, and socio-political influences. It is substantiated that the digitalization of the public sector serves not only as a tool for modernizing administrative processes but also as a crucial factor in ensuring national security, increasing the resilience of state institutions, and enhancing the effectiveness of interaction between the government and the public. The study analyzes contemporary challenges of digital transformation, including cybersecurity issues, the protection of critical information infrastructure, the development of e-government, digital services, and e-democracy mechanisms. Key areas for improving the public governance system under martial law and during the post-war recovery of Ukraine are identified. A comprehensive set of practical measures is proposed to enhance the efficiency of digital governance, develop the digital competencies of public servants, and form an integrated digital ecosystem of public administration.

Keywords: *public governance, digital transformation, digitalization, hybrid threats, cybersecurity, e-government, digital state, digital services, e-democracy, national security.*

REFERENCES

1. Bellamy, C., & Taylor, J.A. (1998). *Governing in the Information Age*. Buckingham: Open University Press.
2. Castells, M. (2010). *The Rise of the Network Society* (2nd ed.). Oxford: Wiley-Blackwell.
3. Dehtiar, O.A. (2021). *Digital transformation of public administration: theory and practice*. Kharkiv: KRI NAPA Publishing.
4. Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New Public Management Is Dead – Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*, 16(3), 467–494. <https://doi.org/10.1093/jopart/mui057>
5. Dziundziuk, V. B. (2022). *Public administration under digitalization conditions*. Kharkiv: Mahistr.
6. European Commission. (2023). *Digital Decade Policy Programme 2030*. Brussels. URL: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade> [in Ukrainian].
7. Horbulin, V.P. (2017). *The world hybrid war: the Ukrainian front*. Kyiv: National Institute for Strategic Studies. [in Ukrainian].

8. Krutii, O.M. (2020). Communicative interaction in public administration. Kharkiv: Mahistr. [in Ukrainian].
9. National Institute of Standards and Technology. (2024). Cybersecurity Framework 2.0. Gaithersburg, MD. URL: <https://www.nist.gov/cyberframework> [in Ukrainian].
10. OECD. (2023). Digital Government Index 2023: Results and Key Findings. Paris: OECD Publishing. URL: <https://www.oecd.org/gov/digital-government> [in Ukrainian].
11. Osborne, D., & Gaebler, T. (1992). Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector. Reading, MA: Addison-Wesley. [in Ukrainian].
12. Pocheptsov, H.H. (2015). Information wars. Kyiv: Kyiv-Mohyla Academy Publishing House. [in Ukrainian].
13. Semenchenko, A.I. (2021). State policy of digital development of Ukraine. Kyiv: NAPA. [in Ukrainian].
14. The Verkhovna Rada of Ukraine. (2012). Code of Civil Protection of Ukraine (Law No. 5403-VI of October 2, 2012). URL: <https://zakon.rada.gov.ua/laws/show/5403-17> [in Ukrainian].
15. The Verkhovna Rada of Ukraine. (2017). On the Basic Principles of Cybersecurity of Ukraine (Law No. 2163-VIII of October 5, 2017). URL: <https://zakon.rada.gov.ua/laws/show/2163-19> [in Ukrainian].
16. The Verkhovna Rada of Ukraine. (2022). On the National Informatization Program (Law No. 2807-IX of December 1, 2022). URL: <https://zakon.rada.gov.ua/laws/show/2807-20>
17. The Cabinet of Ministers of Ukraine. (2021). Strategy of Digital Development, Digital Transformations and Digitalization of Public Administration of Ukraine until 2025 (Order No. 1467-r of November 17, 2021). URL: <https://zakon.rada.gov.ua/laws/show/1467-2021-p>
18. United Nations. (2024). United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. New York: United Nations. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024>
19. West, D. M. (2022). Digital Government: Technology and Public Sector Performance. Princeton: Princeton University Press. <https://doi.org/10.1515/9780691228925>
20. World Bank. (2024). GovTech Maturity Index 2024: Advancing Digital Transformation in the Public Sector. Washington, DC: World Bank. URL: <https://www.worldbank.org/en/programs/govtech>

The article was received by the editors 25.03.2026.

The article is recommended for printing 30.04.2026.

Published 30.05.2026.