УДК 004.056:351:355.4
DOI https://doi.org/10.32782/cuj-2026-1-1

Білик Олена Іванівна
доктор наук з державного управління, професор,
професор кафедри адміністративного та фінансового менеджменту
Національного університету «Львівська політехніка»
Scopus Author ID: 56529456800
ResearcherID: R-7998-2017
ORCID: 0000-0002-7110-7257

Дорош Ірина Миронівна
доктор філософії з публічного управління та адміністрування,
доцент кафедри адміністративного та фінансового менеджменту
Національного університету «Львівська політехніка»
Scopus Author ID: 57202648740
ResearcherID: R-8690-2017
ORCID: 0000-0003-1394-5639

НАПРЯМИ ПІДВИЩЕННЯ БЕЗПЕКИ ЦИФРОВИХ ПУБЛІЧНИХ СЕРВІСІВ ЗА УМОВ ВОЄННИХ РИЗИКІВ

У статті актуалізовано проблематику забезпечення стійкості та безпеки цифрових публічних сервісів в умовах повномасштабної збройної агресії та гібридних загроз. Досліджено трансформацію безпекового середовища функціонування державних цифрових платформ під впливом ескалації кіберпротистояння та фізичного знищення інфраструктури. На основі аналізу емпіричних даних Держспецзв'язку та звітів Microsoft констатовано критичне зростання кількості та складності кібератак на органи публічної влади, що вимагає перегляду традиційних підходів до захисту інформації. Обґрунтовано необхідність переходу від реактивних моделей кіберзахисту до предиктивних стратегій, що базуються на використанні штучного інтелекту та автоматизації процесів реагування (SOAR). Окрему увагу приділено феномену «цифрових посольств» (Data Embassies) та екстериторіальності даних як механізму забезпечення цифрового суверенітету та безперервності державного управління через використання хмарних середовищ країн-партнерів. Проаналізовано когнітивний вимір безпеки, де довіра громадян до цифрових сервісів розглядається як критичний елемент захисту від інформаційно-психологічних операцій ворога. Результатом дослідження є розроблення та обґрунтування багатовимірного механізму підвищення безпеки цифрових публічних сервісів, який базується на синергії чотирьох стратегічних вимірів: нормативно-правового, організаційно-управлінського, технологічного та інституційного. Нормативно-правовий вимір передбачає адаптацію законодавства до умов воєнного часу та імплементацію міжнародних стандартів як обов'язкових вимог. Організаційно-управлінський вимір фокусується на впровадженні адаптивного управління, створенні міжвідомчих коаліцій та залученні громадськості до тестування систем захисту (participatory cybersecurity). Технологічний компонент базується на архітектурі «нульової довіри», кіберрезильєнтності та використанні AI для моніторингу загроз. Інституційний вимір пропонує створення координаційних центрів кібербезпеки та стратегій відновлення даних. Доведено, що інтеграція цих складників дає змогу створити стійку екосистему надання публічних послуг, здатну функціонувати в умовах перманентних кризових ситуацій

Ключові слова: *цифрові публічні сервіси, кіберрезильєнтність, воєнні ризики, цифрові посольства (Data Embassies), Zero-Trust Architecture, адаптивне управління, цифровий суверенітет.*

Bilyk O. I., Dorosh I. M. Directions for enhancing the security of digital public services under war risks

The article addresses the issues of ensuring the resilience and security of digital public services under conditions of full-scale armed aggression and hybrid threats. The transformation of the security environment for the functioning of state digital platforms under the influence of escalating cyber confrontation and physical destruction of infrastructure is investigated. Based on the analysis of empirical data from the SSSCIP and Microsoft reports, a critical increase in the number and complexity of cyberattacks on public authorities is stated, which requires a revision of traditional approaches to information protection. The authors substantiate the necessity of transitioning from reactive cyber defense models to predictive strategies based on the use of artificial intelligence and the automation of response processes (SOAR). Particular attention is paid to the phenomenon of "Data Embassies" and data extraterritoriality as a mechanism for ensuring digital sovereignty and the continuity of public administration through the use of cloud environments of partner countries. The cognitive dimension of security is analyzed, where citizens' trust in digital services is considered a critical element of protection against the enemy's information-psychological operations. The result of the study is the development and substantiation of a multidimensional mechanism for enhancing the security of digital public services, which is based on the synergy of four strategic dimensions: regulatory-legal, organizational-managerial, technological, and institutional. The regulatory-legal dimension provides for the adaptation of legislation to wartime conditions and the implementation of international standards as mandatory requirements. The organizational-managerial dimension focuses on the implementation of adaptive governance, the creation of interagency coalitions, and the involvement of the public in testing protection systems (participatory cybersecurity). The technological component is based on the Zero Trust architecture, cyber resilience, and the use of AI for threat monitoring. The institutional dimension proposes the creation of cybersecurity coordination centers and data recovery strategies. It is proven that the integration of these components allows for the creation of a resilient ecosystem for providing public services, capable of functioning under conditions of permanent crisis situations.

Key words: *digital public services, cyber resilience, war risks, Data Embassies, Zero-Trust Architecture, adaptive governance, digital sovereignty.*

Вступ. Цифровізація публічних сервісів упродовж останнього десятиліття стала одним із основних напрямів модернізації системи публічного управління, спрямованих на підвищення доступності, прозорості та ефективності взаємодії держави з громадянами. Водночас повномасштабне вторгнення росії в Україну, гібридні конфлікти та ескалація кіберпротистояння істотно трансформували безпекове середовище функціонування цифрових публічних сервісів, актуалізувавши проблему їх стійкості, захищеності та безперервності надання в умовах кризових ситуацій. Воєнні ризики суттєво підвищують уразливість цифрової інфраструктури органів публічної влади, зокрема через зростання кількості кібератак, порушення роботи критичних інформаційних систем, обмеження доступу до мережевих ресурсів та загрози цілісності й конфіденційності публічних даних. За таких умов цифрові публічні сервіси перестають бути виключно інструментом підвищення управлінської ефективності та набувають статусу елементів національної безпеки і резильєнтності держави.

Матеріали і методи. Методологічну основу дослідження становить міждисциплінарний підхід, що поєднує інституційний, системний та ризик-орієнтований аналіз безпеки цифрових публічних сервісів в умовах воєнних і гібридних загроз. Матеріальною базою дослідження слугують наукові публікації українських і зарубіжних авторів, а також міжнародні аналітичні та урядові звіти, які репрезентують сучасні теоретико-прикладні підходи до цифрової трансформації, кібербезпеки та управління резильєнтністю державних інформаційних систем. Концептуальні засади аналізу безпекових ризиків цифрових публічних сервісів сформовано з урахуванням положень Global Risks Report 2026, підготовленого експертними колективами World Economic Forum [1], у якому воєнні конфлікти, кіберзагрози, дезінформація та фрагментація цифрового простору розглядаються як взаємопов'язані системні ризики. Зазначений звіт використано для інтерпретації зовнішніх макроризиків, що впливають на стабільність функціонування державних цифрових платформ у кризових умовах. Національний вимір проблематики безпеки цифрових публічних сервісів досліджено на основі праць українських науковців. Нормативно-правові аспекти захисту публічних інформаційних сервісів у цифровій державі проаналізовано

з урахуванням підходів О. Мінька [2], тоді як базові принципи інформаційної безпеки в системі електронного урядування та природу кіберзагроз систематизовано на основі досліджень М. Кутової [3]. Галузеві ризики цифровізації, зокрема у сфері публічних фінансів, розкрито у роботах С. Качули [4], що дало змогу конкретизувати уразливості критичних сегментів цифрового публічного управління. Інституційний контекст забезпечення інформаційної безпеки у системі публічного управління та перспективи її розвитку проаналізовано з опорою на наукові напрацювання М. Нагорняка [5], тоді як інституційні обмеження та адаптаційні механізми цифрової трансформації в Україні узагальнено з урахуванням висновків Д. Солодовніка [6]. Методичні підходи до формування ефективної кібербезпекової політики доповнено результатами досліджень Г. Нґобені та М. Ва Нконголо [7], які акцентують на інтеграції технічної експертизи та публічної участі у процесі вироблення рішень, а також підтвердження необхідності пошуку шляхів забезпечення мережевої стійкості та цифрового суверенітету в умовах російсько-української війни [8]. У практичному вимірі дослідження спирається на положення Урядового плану дій у сфері кібербезпеки [9], розробленого урядом Великої Британії, який використано для порівняльної оцінки інституційних та технологічних механізмів підвищення кіберрезильєнтності державних цифрових платформ і можливостей їх адаптації до національного контексту.

Попри значну кількість досліджень, присвячених цифровій трансформації публічного управління та проблемам кібербезпеки, питання комплексного формування та впровадження механізмів підвищення безпеки цифрових публічних сервісів саме в умовах воєнних ризиків залишається недостатньо систематизованим у науковому дискурсі.

Метою статті є обґрунтування механізму підвищення безпеки цифрових публічних сервісів за умов воєнних ризиків, а також визначення можливостей їх імплементації у практику публічного управління з метою забезпечення стійкості та безперервності надання публічних послуг.

Результати. Глибинний аналіз трансформації архітектури безпеки цифрових публічних сервісів в умовах довготривалих воєнних загроз дає змогу констатувати перехід до високотехнологічної моделі захисту, яка базується на інтелектуалізації процесів та екстериторіальності даних. Емпіричним підтвердженням ескалації загроз є статистика Держспецзв'язку: якщо у 2021 р. було зафіксовано близько 900 кіберінцидентів, то у перший рік повномасштабного вторгнення (2022) ця цифра зросла у три рази – до понад 2 100 інцидентів [10], а у 2023–2024 рр. стабілізувалася на рівні 2 500+ атак щорічно, змінивши при цьому якісну структуру [10]. Згідно зі звітом Microsoft щодо цифрової оборони [12], спостерігається чітка кореляція між кібердарами по енергетичній інфраструктурі та піковими навантаженнями на цифрові сервіси. Близько 40 % усіх деструктивних атак були спрямовані саме на організації критичної інфраструктури, що підтверджує тезу про використання кіберпростору як повноцінного театру воєнних дій. При цьому час підготовки атаки скоротився: якщо раніше хакери могли перебувати в системі місяцями (dwell time), то тепер деструктивні дії часто розпочинаються через 48–72 години після первинного проникнення, що вимагає миттєвої реакції, недосяжної для людини-оператора Таким чином, динаміка кіберінцидентів свідчить, що кількісне зростання автоматизованих атак унеможливлює ефективне реагування виключно силами людського ресурсу, що актуалізувало впровадження платформ автоматизації та оркестрації безпеки (SOAR – Security Orchestration, Automation and Response). Важливість цього переходу полягає у зміні вектору від реактивного захисту периметра до предиктивної протидії: алгоритми штучного інтелекту та машинного навчання (ML) дають змогу аналізувати патерни мережевої поведінки в режимі реального часу, виявляючи аномалії, що передують атаці, ще до моменту її активної фази. Це дає змогу скоротити час виявлення загрози та час реагування до мінімальних значень, автоматично ізолюючи скомпрометовані сегменти без зупинки роботи всієї екосистеми публічних послуг. Таким чином, технологічна

резильєнтність досягається не збільшенням штату адміністраторів, а інтеграцією когнітивних обчислень у контур кібербезпеки.

Паралельно з технологічною модернізацією дослідження виявило формування нового міжнародно-правового феномену забезпечення безперервності державного управління – концепції «цифрових посольств» (Data Embassies). Цей підхід, що еволюціонував із практики хмарного резервування, набув ознак інституційної зрілості завдяки адаптації Україною досвіду Естонії та нормативному врегулюванню можливості зберігання державних реєстрів за межами національної юрисдикції. За інформацією Міністерства цифрової трансформації, у період 2022–2024 рр. у хмарні середовища (AWS, Microsoft Azure, Google Cloud) було успішно перенесено понад 100 державних реєстрів та критичних баз даних. За оцінками експертів, це дало змогу зберегти 100 % цілісність даних попри фізичне пошкодження або знеструмлення понад 20 % наземних дата-центрів унаслідок ракетних обстрілів. Економічний ефект від співпраці з техногігантами (зокрема, надання безкоштовних хмарних послуг компанією Amazon Web Services у 2022 р.) оцінюється у понад 75 млн доларів США [13], що свідчить про важливість міжнародного ресурсного забезпечення для кіберстійкості країни, яка воює. Аналіз правової природи цього механізму показує, що йдеться не лише про технічний хостинг даних на серверах країн-партнерів [14] (зокрема, Польщі), а й про поширення державного суверенітету на цифрову інфраструктуру, розташовану за кордоном. Такий механізм гарантує, що дані та інформаційні системи користуються імунітетом, аналогічним дипломатичному, що убезпечує їх не лише від фізичного знищення внаслідок бойових дій, а й від юридичних ризиків утручання третьої сторони. Це дає змогу стверджувати про виникнення моделі «розподіленого суверенітету», де цілісність державних баз даних забезпечується міжнародними угодами, що є критичним чинником виживання інституцій в умовах тотальної війни.

Водночас комплексний аналіз безпекового ландшафту доводить, що захист цифрових сервісів не обмежується технічними та правовими заходами, а охоплює когнітивний вимір. В умовах гібридної агресії цифрові платформи (на прикладі екосистеми «Дія») стають об'єктом інформаційно-психологічних операцій, спрямованих на підрив довіри населення до державних інституцій. Сприйняття громадянами безпеки сервісу є таким же критичним показником, як і криптографічна стійкість: успішна дезінформаційна кампанія (наприклад, щодо фейкових витоків даних або незаконних повісток через застосунок) здатна делегітимізувати цифровий інструмент швидше, ніж DDoS-атака. Отже, забезпечення когнітивної безпеки вимагає інтеграції в інтерфейси публічних послуг механізмів проактивної комунікації, верифікації контенту та цифрової едукації користувачів. Це обґрунтовує необхідність розгляду безпеки цифрових публічних сервісів як соціотехнічного феномену, де довіра користувача є невід'ємним складником архітектури захисту, а протидія соціальній інженерії стає пріоритетним завданням державного менеджменту. Проте опитування, проведені Київським міжнародним інститутом соціології (КМІС), демонструють, що рівень довіри до цифрових держпослуг залишається стабільно високим (понад 70 %) [15], що перевищує довіру до багатьох традиційних офлайн-інституцій. Це свідчить про те, що вибрана стратегія проактивної комунікації та швидкого відновлення сервісів після збоїв (resilience) нівелювала ефект когнітивних атак.

Отримані результати дослідження демонструють, що безпека цифрових публічних сервісів не може розглядатися як ізольована категорія, обмежена лише технологічними або правовими заходами. Умови воєнних та гібридних загроз вимагають системного підходу, який інтегрує різні рівні управлінських рішень, технологічних інструментів та нормативно-правових регуляцій. Аналіз міжнародних кейсів, зокрема адаптивного управління платформою «Дія», даних Global Risks Report 2026 [1] та урядових планів кібербезпеки показує, що ефективність заходів безпеки визначається не лише наявністю технічних рішень, а й здатністю організацій швидко адаптуватися до нових ризиків, координувати дії між різними суб'єктами і забезпечувати стійкість сервісів у кризових умовах.

Така системна природа безпеки цифрових публічних сервісів зумовлює необхідність виділення окремих взаємопов'язаних вимірів, що дають змогу інтегрувати нормативно-правові рамки, організаційно-управлінські механізми, технологічні засоби та інституційні інструменти координації. Кожен із цих вимірів виступає надзвичайно важливим елементом комплексної моделі кіберрезильєнтності, забезпечуючи синергію дій для підтримки безперервності цифрових сервісів у складних і динамічних умовах воєнного часу. З огляду на це, ефективна система захисту має ґрунтуватися на синергії різних підходів. Систематизацію основних інструментів кіберстійкості, що охоплює нормативні, організаційні, технологічні та інституційні виміри, наведено в табл. 1.

Представлений багатовимірний механізм демонструє, що підвищення безпеки цифрових

Таблиця 1

Багатовимірний механізм підвищення безпеки цифрових публічних сервісів

Вимір	Інструмент	Опис та імплементація	Очікувані результати
Нормативно-правовий	Адаптація законодавства до умов війни	Розроблення та оновлення актів, що специфічно регулюють захист інформаційних систем від кіберзагроз в умовах воєнного стану та фізичного знищення інфраструктури	Підвищення правової спроможності держави реагувати на кібератаки та збройні загрози; юридичне забезпечення безперервності сервісів
	Стандартизація та комплаєнс	Упровадження міжнародних стандартів (GDPR, ISO 27001, NIST) як обов'язкових вимог до цифрової трансформації, а не рекомендаційних	Уніфікація процесів безпеки, мінімізація технічних уразливостей, підвищення довіри користувачів до сервісів
	Регуляторна координація	Інституційне (законодавче) закріплення протоколів взаємодії між центральною владою та локальними громадами для юридичної легітимності оперативного реагування	Швидке та законне реагування на інциденти, зменшення хаосу у кризових ситуаціях
Організаційно-управлінський	Адаптивне управління (Agile Governance)	Відхід від жорстких інструкцій до постійного моніторингу, оцінки ризиків і швидкої корекції управлінських процесів під час криз	Зниження часу реагування на загрози, гнучке управління сервісами в умовах нестабільності
	Міжвідомчі коаліції	Створення оперативних штабів та коаліцій для забезпечення безперервності надання публічних послуг навіть під час масованих атак	Синхронізація дій державних і приватних структур; підтримка безперервності ключових цифрових сервісів
	Participatory Cybersecurity	Залучення громадянського суспільства («білих хакерів», IT-спільноти) та експертних структур до тестування вразливостей (bug bounty) та розроблення заходів захисту	Підвищення практичної ефективності заходів кіберзахисту та швидке усунення уразливостей
Технологічний	Zero-Trust Architecture	Перехід від захисту периметра до моделі «нульової довіри», де кожна транзакція та запит на доступ проходять багаторівневу перевірку	Зменшення ризику несанкціонованого доступу та компрометації даних, підвищення кіберрезильєнтності
Інституційний	Координаційні центри кібербезпеки	Створення національних та регіональних центрів кібербезпеки для інтеграції державних органів, операторів цифрових платформ та громадських організацій.	Підвищення узгодженості дій усіх стейкхолдерів; ефективне реагування на кризові ситуації.
	Стратегії цифрового суверенітету	Розроблення національних планів і політик щодо контролю цифрової інфраструктури, відновлення даних і управління ризиками у воєнних умовах	Забезпечення національної автономії цифрових сервісів; зменшення залежності від зовнішніх постачальників та ризиків кібератак
	Моніторинг та оцінка ефективності	Упровадження систем регулярного аудиту, моніторингу та аналітичних звітів для оцінки ефективності заходів безпеки та вдосконалення процесів кіберрезильєнтності	Своєчасне виявлення слабких місць, оптимізація процедур безпеки, підвищення загальної стійкості цифрових сервісів

публічних сервісів в умовах воєнних та гібридних загроз потребує інтегрованого підходу, який одночасно охоплює нормативно-правові, організаційно-управлінські, технологічні та інституційні виміри.

Нормативно-правовий вимір створює правову основу та стандартизацію, що дає змогу оперативно реагувати на кіберзагрози та забезпечує юридичну легітимність дій органів влади. Організаційно-управлінський вимір формує гнучкі механізми адаптивного управління, включаючи міжвідомчі коаліції та участь громадянського суспільства, що забезпечує ефективну координацію дій під час кризових ситуацій. Технологічний вимір забезпечує технічну безпеку та стійкість сервісів, упроваджуючи сучасні рішення, такі як Zero-Trust-архітектура та багаторівневі системи моніторингу та контролю доступу.

Інституційний вимір, доданий до моделі, забезпечує системну координацію та стратегічне управління кібербезпекою на національному та регіональному рівнях. Це включає створення координаційних центрів кібербезпеки, розроблення стратегій цифрового суверенітету та постійний моніторинг ефективності впроваджених заходів. Інтеграція цього виміру дає змогу забезпечити синергію між технічними, нормативними та управлінськими компонентами, підвищуючи загальну стійкість цифрових платформ у воєнних умовах.

Очікувані результати впровадження таких механізмів підтверджують, що системна багатовимірна модель дає змогу значно зменшити уразливість цифрових публічних сервісів, підвищити швидкість реагування на загрози та забезпечити безперервність надання послуг. Таким чином, багатовимірна структура механізмів формує ефективну основу для стратегічного управління кібербезпекою державних цифрових платформ і може бути імплементована як в умовах воєнного часу, так і в рамках довгострокових планів цифрової трансформації держави.

Висновки. Дослідження засвідчило, що підвищення безпеки цифрових публічних сервісів у умовах воєнних ризиків вимагає багатовимірного підходу. Такий механізм забезпечує синергію між законодавством, управлінськими процесами, технічними рішеннями та інституційною координацією, що підвищує кіберрезильєнтність платформ і гарантує безперервність надання публічних послуг.

Перспектива подальших досліджень пов'язана з розробленням методик оцінки ефективності впроваджених заходів, моделюванням сценаріїв кіберзагроз та вдосконаленням інтегрованих систем управління цифровою безпекою, що дасть змогу адаптувати механізми під нові технологічні та воєнні виклики.

Література

1. Global risks report 2026 / World Economic Forum. 2026. URL: https://www.weforum.org/publications/global-risks-report-2026/ (дата звернення: 05.01.2026).

2. Мінько О. Нормативно-правове регулювання забезпечення безпеки публічних інформаційних сервісів в Україні. *Law. State. Technology*. 2024. № 2. С. 30–34. URL: https://doi.org/10.32782/LST/2024-2-6 (дата звернення: 06.01.2026).

3. Кутова М. А. Основи інформаційної безпеки в системі електронного урядування. *Economic Synergy*. 2024. № 1. С. 20–30. URL: https://doi.org/10.53920/ES-2024-1-2 (дата звернення: 07.01.2026).

4. Качула С. Кібербезпека у сфері публічних фінансів. *Економіка та суспільство*. 2025. № 77. URL: https://doi.org/10.32782/2524-0072/2025-77-69 (дата звернення: 09.01.2026).

5. Нагорняк М. М. Інформаційна безпека у системі публічного урядування: виклики та перспективи. *Дніпровський науковий часопис публічного урядування, психології, права*. 2024. № 1. URL: https://doi.org/10.51547/ppp.dp.ua/2024.1.10 (дата звернення: 10.01.2026).

6. Солодовнік Д. Цифрові виклики та інституційні обмеження в системі публічного урядування України. *Публічно-управлінські та цифрові практики*. 2025. Вип. 2(5). URL: https://doi.org/10.31673/2786-7412.2025.028587 (дата звернення: 12.01.2026).

7. Ngobeni H., Wa Nkongolo M. Integrating public input and technical expertise for effective cybersecurity policy formulation. *arXiv*. 2025. URL: https://arxiv.org/abs/2512.08575 (дата звернення: 13.01.2026).

8. Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine / M.S. Gustafsson et al. *Government Information Quarterly*. 2025. Vol. 42, Iss. 3. Art. 102056. URL: https://doi.org/10.1016/j.giq.2025.102056 (дата звернення: 15.01.2026).

9. Government cyber action plan / Department for Science, Innovation and Technology. UK Government. 2026. URL: https://www.gov.uk/government/publications/government-cyber-action-plan/government-cyber-action-plan (дата звернення: 16.01.2026).

10. Russia's cyber tactics: Lessons learned in 2022 – SSSCIP analytical report on the year of Russia's full-scale cyberwar against Ukraine / State Service of Special Communications and Information Protection of Ukraine. 2023. URL: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine (дата звернення: 17.01.2026).

11. Artemchuk O. Number of cyberattacks on Ukraine increased by 70% in past year. *Ukrainska Pravda*. 2025. 9 Jan. URL: https://www.pravda.com.ua/eng/news/2025/01/09/7492671/ (дата звернення: 18.01.2026).

12. Microsoft digital defense report 2024 / Microsoft. 2024. URL: https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 (дата звернення: 19.01.2026).

13. Amazon Web Services надає Україні підтримки на 75 млн доларів на хмарні технології, які допомагають стабільно працювати цифровій державі та економіці / Міністерство цифрової трансформації України. 2022. 1 грудня. URL: https://kolrda.gov.ua/news/mintsyfry-amazon-web-services-nadaye-ukrayini-pidtrymky-na-75-mln-dolariv-na-khmarni-tekhnolohiyi/ (дата звернення: 20.01.2026).

14. Мельник О. Особливості організації діяльності хмарних сервісів в Україні: Нове правове поле та можливості для глобальних провайдерів. *Golaw*. 2025. 5 травня. URL: https://golaw.ua/ua/insights/publication/osoblivosti-organizacziyi-diyalnosti-hmarnih-servisiv-v-ukrayini-nove-pravove-pole-ta-mozhlivosti-dlya-globalnih-provajderiv/ (дата звернення: 21.01.2026).

15. Українці стали більш задоволеними онлайн-послугами: КМІС презентував дослідження / Міністерство цифрової трансформації України. 2025. 27 січня. URL: https://thedigital.gov.ua/news/technologies/ukraintsi-stali-bilsh-zadovolenimi-onlayn-poslugami-kmis-prezentuvav-doslidzhennya (дата звернення: 22.01.2026).

References

1. World Economic Forum. (2026). *Global risks report 2026*. Retrieved from https://www.weforum.org/publications/global-risks-report-2026/ [in English].

2. Minko, O. (2024). Normatyvno-pravove rehuliuvannia zabezpechennia bezpeky publichnykh informatsiinykh servisiv v Ukraini [Regulatory and legal regulation of ensuring the security of public information services in Ukraine]. *Law. State. Technology, (2)*, 30–34. https://doi.org/10.32782/LST/2024-2-6 [in Ukrainian].

3. Kutova, M. A. (2024). Osnovy informatsiinoi bezpeky v systemi elektronnoho uriaduvannia [Fundamentals of information security in the electronic governance system]. *Economic Synergy, (1)*, 20–30. https://doi.org/10.53920/ES-2024-1-2 [in Ukrainian].

4. Kachula, S. (2025). Kyberbezpeka u sferi publichnykh finansiv [Cybersecurity in the sphere of public finances]. *Ekonomika ta suspilstvo*, (77). https://doi.org/10.32782/2524-0072/2025-77-69 [in Ukrainian].

5. Nahorniak, M. M. (2024). Informatsiina bezpeka u systemi publichnoho uriaduvannia: Vyklyky ta perspektyvy [Information security in the public administration system: Challenges and prospects]. *Dniprovskyi naukovyi chasopys publichnoho uriaduvannia, psykholohii, prava, (1)*. https://doi.org/10.51547/ppp.dp.ua/2024.1.10 [in Ukrainian].

6. Solodovnik, D. (2025). Tsyfrovi vyklyky ta instytutsiini obmezennia v systemi publichnoho uriaduvannia Ukrainy [Digital challenges and institutional limitations in the public administration system of Ukraine]. *Publichno-upravlinski ta tsyfrovi praktyky, 2*(5). https://doi.org/10.31673/2786-7412.2025.028587 [in Ukrainian].

7. Ngobeni, H., & Wa Nkongolo, M. (2025). *Integrating public input and technical expertise for effective cybersecurity policy formulation*. arXiv. Retrieved from https://arxiv.org/abs/2512.08575 [in English].

8. Gustafsson, M. S., Matveieva, O. Yu., Wihlborg, E., Borodin, Ye., Mamatova, T. V., & Kvitka, S. M. (2025). Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine. *Government Information Quarterly, 42*(3), Article 102012. https://doi.org/10.1016/j.giq.2025.102056 [in English].

9. Department for Science, Innovation and Technology. (2026). *Government cyber action plan*. UK Government. Retrieved from https://www.gov.uk/government/publications/government-cyber-action-plan/government-cyber-action-plan [in English].

10. State Service of Special Communications and Information Protection of Ukraine. (2023). *Russia's cyber tactics: Lessons learned in 2022 – SSSCIP analytical report on the year of Russia's full-scale cyberwar against Ukraine*. Retrieved from https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine [in English].

11. Artemchuk, O. (2025, January 9). Number of cyberattacks on Ukraine increased by 70% in past year. *Ukrainska Pravda*. Retrieved from https://www.pravda.com.ua/eng/news/2025/01/09/7492671/ [in English].

12. Microsoft. (2024). *Microsoft digital defense report 2024*. Retrieved from https://www.microsoft.com/en-gb/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 [in English].

13. Ministry of Digital Transformation of Ukraine. (2022, December 1). *Amazon Web Services nadaie Ukraini pidtrymky na 75 mln dolariv na khmarni tekhnolohii, yaki dopomahaiut stabilno pratsiuvaty tsyfrovii derzhavi ta ekonomitsi* [Amazon Web Services provides Ukraine with support worth USD 75 million for cloud technologies, helping maintain stable digital state and economy]. Retrieved from https://kolrda.gov.ua/news/mintsyfry-amazon-web-services-nadaye-ukrayini-pidtrymky-na-75-mln-dolariv-na-khmarni-tekhnolohiyi/ [in Ukrainian].

14. Melnyk, O. (2025, May 5). *Osoblyvosti orhanizatsii diialnosti khmarnykh servisiv v Ukraini: Nove pravove pole ta mozhlyvosti dlia hlobalnykh provayderiv* [Peculiarities of organizing the activities of cloud services in Ukraine: New legal fields and opportunities for cloud providers]. Golaw. Retrieved from https://golaw.ua/ua/insights/publication/osoblivosti-organizacziyi-diyalnosti-hmarnih-servisiv-v-ukrayini-nove-pravove-pole-ta-mozhlivosti-dlya-globalnih-provajderiv/ [in Ukrainian].

15. Ministry of Digital Transformation of Ukraine. (2025, January 27). *Ukraintsi staly bilsh zadovolenymy onlain posluhamy: KMIS prezentuvav doslidzhennia* [Ukrainians became more satisfied with online services: KMIS presented research]. Retrieved from https://thedigital.gov.ua/news/technologies/ukraintsi-stali-bilsh-zadovolenimi-onlayn-poslugami-kmis-prezentuvav-doslidzhennya [in Ukrainian].

Дата першого надходження статті до видання: 25.01.2026
Дата прийняття статті до друку після рецензування: 23.02.2026
Дата публікації (оприлюднення) статті: 20.04.2026