УДК 351:004.9:355.01(477)

https://doi.org/10.62664/cpa.2026.01.03

Євген БЕРЛАДИНЮК,
здобувач вищої освіти
за третім (освітньо-науковим) рівнем вищої освіти,
Івано-Франківський національний технічний університет нафти і газу
ORCID ID http://orcid.org/0009-0004-5339-4792

ВПЛИВ ЦИФРОВІЗАЦІЇ УКРАЇНИ В УМОВАХ ВІЙНИ НА ДЕРЖАВНЕ УПРАВЛІННЯ В БЕЗПЕКОВИХ ВИМІРАХ

У статті досліджено трансформацію цифрової державності України в умовах повномасштабної війни крізь призму міжнародних відносин, державного управління та національної безпеки. Доведено, що після 24 лютого 2022 року цифровізація перестала бути лише інструментом адміністративної зручності й стала критичним елементом державної спроможності, інституційної неперервності та безпекової резильєнтності. На підставі аналізу українського законодавства, офіційних урядових матеріалів, документів ЄС, звітів міжнародних організацій та фахової академічної літератури обґрунтовано, що українська модель цифрової трансформації у воєнний період базується на поєднанні трьох функціональних контурів: сервісного, інфраструктурно-реєстрового та кібербезпекового. У сервісному контурі показано, що масштабування екосистеми Дія та запуск нових воєнних і відновлювальних сервісів – для ВПО, власників пошкодженого житла, ветеранів, сімей військовослужбовців і громадян, які користуються міжнародними механізмами фіксації збитків, – забезпечили зменшення транзакційних витрат, швидкість рішень і підвищення доступності держави в кризовому середовищі. В

інфраструктурно-реєстровому контурі виявлено вирішальну роль законодавства про публічні електронні реєстри, хмарні послуги, електронну ідентифікацію та довірчі послуги, а також хмарної міграції критичних державних даних до дата-центрів у ЄС і США, що знизило ризики фізичного знищення, втрати доступності та руйнування державних даних унаслідок кінетичних ударів. У безпековому контурі встановлено, що російська кіберкампанія проти України еволюціонувала від переважно деструктивних атак 2022 року до складніших шпигунських, фішингових, supply-chain та багатовекторних операцій 2023–2025 років; відповідно, кіберзахист трансформувався в багаторівневу систему співпраці держави, приватного сектору та міжнародних партнерів. Окремо проаналізовано євроінтеграційний вимір цифровізації: асоціацію України до Digital Europe Programme, наближення до eIDAS та eIDAS 2.0, імплементацію підходів NIS/NIS2, розвиток проєктів DT4UA та EU4DigitalUA, а також політичне рішення 2025 року про включення України до роумінгової зони ЄС із 2026 року. Обґрунтовано, що цифровізація в умовах війни стала формою стратегічної адаптації державного управління, а її дальший розвиток має відбуватися як безпекова політика, а не лише як адміністративна інновація. Стаття доводить потребу переходу від «цифровізації послуг» до «цифрової державної спроможності», де сумісність із acquis ЄС, стійкість телеком-інфраструктури, реєстрова цілісність, кіберзахист, інклюзивність і захист даних є взаємопов'язаними складниками одного управлінського проєкту.

Ключові слова: *цифровізація; цифрова держава, електронне урядування, державне управління, національна безпека, кібербезпека, резильєнтність, електронні реєстри, хмарні послуги, європейська інтеграція, воєнний стан.*

Yevhen BERLADYNIUK,
PhD student
(third, educational and research level of higher education),
Ivano-Frankivsk National Technical University of Oil and Gas
ORCID ID http://orcid.org/0009-0004-5339-4792

THE IMPACT OF UKRAINE'S DIGITALIZATION IN WAR CONDITIONS ON STATE ADMINISTRATION IN SECURITY DIMENSIONS

The article examines the transformation of Ukraine's digital statehood in full-scale war conditions through the prism of international relations, public administration, and national security. It is proven that after February 24, 2022, digitalization ceased to be just a tool of administrative convenience and became a critical element of state capacity, institutional continuity, and security resilience. Based on the analysis of Ukrainian legislation, official government materials, EU documents, reports of international organizations, and professional academic literature, it is substantiated that the Ukrainian model of digital transformation in wartime is based on a combination of three functional contours: service, infrastructure-registration, and cybersecurity. The service circuit shows that the scaling of the Diya ecosystem and the launch of new military and recovery services – for IDPs, owners of damaged housing, veterans, families of military personnel, and citizens using international loss-fixing mechanisms – have reduced transaction costs, speeded up decisions, and increased the accessibility of the state in a crisis environment. The infrastructure and registry circuit reveals the crucial role of legislation on public electronic registries, cloud services, electronic identification, and trust services, as well as cloud migration of critical state data to data centers in the EU and the US, which reduced the risks of physical destruction, loss of accessibility, and destruction of state data due to kinetic strikes. The security circuit establishes that

the Russian cyber campaign against Ukraine has evolved from predominantly destructive attacks in 2022 to more complex espionage, phishing, supply-chain, and multi-vector operations in 2023–2025; accordingly, cyber defense has been transformed into a multi-level system of cooperation between the state, the private sector, and international partners. The European integration dimension of digitalization is separately analyzed: Ukraine's association with the Digital Europe Programme, approximation to eIDAS and eIDAS 2.0, implementation of NIS/NIS2 approaches, development of the DT4UA and EU4DigitalUA projects, as well as the 2025 political decision to include Ukraine in the EU roaming area from 2026. It is substantiated that digitalization in wartime has become a form of strategic adaptation of public administration, and its further development should take place as a security policy, and not only as an administrative innovation. The article proves the need to transition from «digitalization of services» to «digital state capacity», where compatibility with the EU acquis, stability of telecom infrastructure, register integrity, cyber defense, inclusiveness, and data protection are interrelated components of one management project.

Keywords: *digitalization; digital state, e-government, public administration, national security, cybersecurity, resilience, electronic registries, cloud services, European integration, martial law.*

Постановка проблеми. Наукова проблема полягає в тому, що в українському дискурсі цифровізація часто описується або як технократичне реформаторство, або як сукупність окремих сервісних рішень, тоді як війна висунула на перший план її безпекову, інституційну та міжнародно-політичну функції. Фактично йдеться про зміну предмета аналізу: від е-урядування як каналу надання послуг до цифрової державності як механізму виживання держави, збереження суверенітету даних, швидкого реагування та інтеграції до європейського цифрового простору. Саме ця багатовимірність потребує

міждисциплінарного підходу, релевантного для міжнародних відносин, публічного управління та національної безпеки [1].

Аналіз останніх досліджень і публікацій. У національній академічній літературі проблематика електронного урядування та цифровізації публічного адміністрування в умовах війни вже окреслено, проте здебільшого у фрагментований спосіб. Є. Гульчук акцентує увагу на Дії як інструменті електронного урядування та пов'язує її розвиток із доступністю послуг, прозорістю та модернізацією публічного управління. Л. Самойленко та А. Тихомирова аналізують диджиталізацію адміністративних послуг у воєнний час на прикладі сервісу Дія та наголошують на адаптивному характеру цифрової екосистеми до умов правового режиму воєнного стану. С. Чукут та Є. Карпенко досліджують організацію надання електронних послуг у воєнних умовах, розглядаючи інституційну роль профільних органів і практичні прояви впливу війни на е-сервіси.

В англомовній літературі домінують два напрями. Перший – кібербезпековий: Роман Колодій пояснює стійкість України до російської кіберагресії через інституційне навчання та адаптацію, а Ліліан Аксон та співавт. наголошують на значенні публічно-приватних ініціатив у кіберзахисті. Другий – міжнародно-правовий та стратегічний: дослідження К. Айхензеер звертає увагу на місце кібератак у сучасній війні та обмеження класичних правових інтерпретацій у випадку України. Проте навіть ці праці рідко поєднують сервіси, реєстри, телеком-інфраструктуру, кібервійну та європейську інтеграцію в єдину рамку аналізу державного управління [2].

Водночас у прикладних та аналітичних звітах картина є повнішою. OECD [16] наголошує, що цифрова доставка послуг в Україні продемонструвала стійкість після початкових збоїв, а Міжнародний союз електрозв'язку фіксує водночас руйнування комунікаційної інфраструктури та адаптивність ІСТ-сектору. Офіційні українські та європейські документи, своєю чергою, дозволяють простежити, як цифрова трансформація переходить у площину

нормативної конвергенції з ЄС, кіберрезильєнтності та відбудови. Саме тому в цій статті пріоритет надано первинним і офіційним джерелам, а академічна література використовується для інтерпретації та теоретичного узагальнення.

Мета статті полягає в тому, щоб концептуалізувати цифровізацію України в умовах війни як процес трансформації державного управління в безпекових вимірах і на цій основі: по-перше, показати зміну функцій цифрових сервісів та інфраструктури у воєнний період; по-друге, оцінити роль кібербезпеки й телекомстійкості; по-третє, розкрити значення співпраці з ЄС для інституційного та правового переналаштування цифрової держави; по-четверте, сформулювати рекомендації державної політики для повоєнного етапу та переговорного процесу з ЄС.

Виклад основного матеріалу. Війна радикально змінила зміст цифрової політики. Якщо до 2022 року центральним питанням було спрощення доступу до послуг та зменшення корупційної ренти, то після вторгнення – забезпечення неперервності функціонування держави під умовами фізичного знищення інфраструктури, масового переміщення людей, кібератак і дефіциту часу на управлінське реагування. Світовий банк разом із Європейською Комісією та ООН у рамках RDNA наголошують на системному характері воєнних руйнувань, а ITU окремо фіксує масштабні пошкодження телекомунікацій, що безпосередньо впливають на доступність цифрових сервісів і зв'язок громадян із державою. Попри це український цифровий сектор продемонстрував високу адаптивність. За профілем ITU, 2023 року в Україні було 8,07 млн фіксованих широкосмугових підключень і 33,4 млн мобільних широкосмугових підключень; загальні доходи від комунікаційних послуг сягнули 130,5 млрд грн, а частка xPON зросла до 41,3%, що віддзеркалює переорієнтацію сектора на енергонезалежніші та стійкіші рішення. Це означає, що війна не просто створила шок, а й прискорила перебудову інфраструктурних пріоритетів у бік стійкості та європейських стандартів підключення [3].

Управлінський сенс цього контексту полягає в тому, що цифровізація стала частиною «держави без фізичної черги». Умовно кажучи, громадянин, який перемістився в межах країни або за кордон, держава, що працює під ризиком ракетних ударів, і міжнародний донор, який потребує прозорого цифрового сліду, одночасно формують попит на ту саму річ – надійну цифрову управлінську інфраструктуру. Саме тому воєнний контекст не є зовнішнім чинником для цифровізації: він є її новим операційним середовищем. Зазначимо, що створення засад сучасної цифрової держави відбулося ще до повномасштабної війни: 2019 року було визначено повноваження профільного міністерства, а також нормативно оформлено Єдиний державний вебпортал електронних послуг. 2021 року ухвалено Закон про публічні електронні реєстри, що зафіксував реєстрову логіку цифрової державності, а законодавство про електронну ідентифікацію та довірчі послуги сформувало базу для юридично значущих дій онлайн. Ці рішення не були периферійними – саме вони створили можливість для швидкого масштабування послуг під час війни [4].

Офіційні підсумки розвитку Дії 2025 року засвідчують, що сервісна логіка зберегла високу динаміку: за час війни в застосунку та на порталі з'явилося понад 70 нових сервісів, а загальна кількість користувачів застосунку досягла 19,8 млн. В урядовій оцінці сукупний ефект Дії за п'ять років визначено у 184 млрд грн заощаджених коштів для громадян і держави; окремо наголошено на економії від цифровізації базових послуг, програм підтримки та будівельних сервісів. Ці цифри варто трактувати не лише як показник зручності, а як індикатор того, що цифрові рішення зменшують адміністративний час, знижують навантаження на фронт-офіси та прискорюють урядове реагування у кризових умовах. У воєнний період найбільш показовими є саме ті сервіси, що поєднують соціальну, правову й відновлювальну функції. Програму єВідновлення зорієнтовано на власників житла, пошкодженого або зруйнованого через бойові дії. Допомога ВПО через Дію забезпечує спрощений доступ до виплат; офіційний гід прямо фіксує модель призначення допомоги на сім'ю, її

строки та розміри. У таких сервісах цифровізація не замінює політику, а переводить її у більш швидкий і масштабований формат виконання. Саме тому Дія в умовах війни перетворилася на платформу реалізації державної соціальної політики, а не тільки на канал отримання довідок.

Критично важливо, що сервісний рівень спирається на глибинну інфраструктуру. У цьому аспекті визначальними стали Закон про хмарні послуги та урядовий порядок 2025 року щодо особливостей надання й використання хмарних послуг для державних інформаційних ресурсів та інформації з обмеженим доступом. Війна показала, що без нормативно дозволеної хмарної моделі неможливо масштабно резервувати реєстри, забезпечувати віддалений доступ і створювати географічно розосереджену архітектуру зберігання даних. Цей вимір робить цифрову інфраструктуру частиною стратегії цивільної оборони держави [5].

Кіберстійкість України формується на перетині правових, технологічних і кооперaційних елементів. Чинний базовий закон про основні засади забезпечення кібербезпеки покладає на уряд функції організації національної системи кібербезпеки, затвердження національного плану реагування, загальних вимог із кіберзахисту критичної інфраструктури та порядку взаємодії суб'єктів реагування на кіберінциденти. Указом 2021 року реалізацію Стратегії кібербезпеки визначено до 2025 року, що створило програмну рамку ще до повномасштабної фази війни [6].

На початку вторгнення пріоритетом російських кібероперацій були деструктивні сценарії. Офіційні матеріали Держспецзв'язку та CERT-UA вказують на хвилю руйнівного ПЗ на кшталт HermeticWiper, IsaacWiper, CaddyWiper, а також на спробу масованої атаки на енергетичний сектор із використанням Industroyer2 і CaddyWiper, яку було попереджено у квітні 2022 року. Звіт за 2022 рік також фіксує, що Sandworm залишався ключовим деструктивним актором у сферах енергетики, логістики, медіа та іншої критичної інфраструктури [7].

Надалі противник змінив акценти. За публічною оцінкою 2025 року, російські хакери перейшли від переважно деструктивних атак до розвідки, збору даних, закріплення в системах і поєднання кібероперацій з інформаційно-психологічними ефектами. У 2023–2024 роках зростає значення фішингових кампаній, атак на месенджери та мобільні пристрої військовиків, компрометації поштових скриньок, експлуатації вразливостей у популярному ПЗ, а також атак на місцеві органи влади. 2025 року CERT-UA повідомляє про середньо близько 15 кіберінцидентів на день і відстеження понад 150 кластерів активності. Ця динаміка свідчить, що війна в кіберпросторі дедалі більше тяжіє до виснаження, інфільтрації та викрадення контекстно цінної інформації.

Показовою була кібератака на мережу «Київстар» у грудні 2023 року, що призвела до блокування основних сервісів одного з найбільших телеком-операторів. Держспецзв'язок трактував її як потужну атаку на інформаційні системи, а у звіті про російські кібероперації ця подія інтерпретується як елемент гібридної війни з виразним ефектом для цивільного населення та координації під час ракетних ударів. Цей кейс показав, що телеком-сектор у сучасній війні є не менш критичним, ніж енергетика: без зв'язку руйнується доступ до послуг, оповіщення, фінансових операцій і частини командно-інформаційних процесів. Водночас українська кіберрезильєнтність ґрунтується не лише на відбитті атак, а й на швидкому відновленні. У звіті Держспецзв'язку за 2025 рік серед ключових чинників названо міграцію критичних державних даних до захищених хмарних середовищ у ЄС і США, створення резервних копій та альтернативних каналів доступу до важливих ресурсів. Це означає, що захист тепер мислиться не виключно через периметр, а через здатність держави працювати навіть після прориву окремих сегментів. У науковому вимірі така логіка відповідає переходу від «безпеки за бар'єром» до «стійкості за проєктуванням» [7].

Європейський вимір цифровізації є для України одночасно ресурсним, нормативним і геополітичним. 2022 року Україну було асоційовано до програми Digital Europe, що дало змогу українським організаціям, бізнесу та публічним

адміністраціям брати участь у конкурсах програми з загальним бюджетом 7,5 млрд євро на 2021–2027 роки. Це рішення важливе не лише як джерело фінансування, а як механізм входження до цифрової політики ЄС у сферах суперкомп'ютерів, AI, цифрових навичок та інноваційних хабів.

Поглиблення інтеграції відбувається і через спеціалізовані програми підтримки. Проєкт DT4UA, що фінансується ЄС і реалізується у співпраці з естонською e-Governance Academy та українськими державними інституціями, мав бюджет 17,4 млн євро на період від листопада 2022 року до грудня 2025 року. За відкритими даними, у межах проєкту було оновлено і запущено понад 150 електронних сервісів, підтримано розвиток Vulyk, е-сервісів, технічних умов сумісності з eIDAS та рішень, що підвищили зручність і безпечність державних сервісів у воєнний час. У попередніх хвилях підтримки ЄС, за даними eGA, з 2016 року сукупний бюджет цифрової допомоги перевищив 51 млн євро [8].

Сфера електронної ідентифікації є особливо показовою. DT4UA та пов'язані з ним ініціативи створили технічні та організаційні передумови для визнання українських електронних довірчих послуг у країнах ЄС. У публічних матеріалах проєкту прямо зазначено, що українські довірчі послуги гармонізовано з вимогами eIDAS, а Diia.Signature може використовуватися у взаємодії з партнерами в ЄС. Крім того, Європейська Комісія 2023 року запустила пілоти EUDI Wallet, до яких залучено також Україну. У перспективі це зменшує бар'єри для транскордонних цифрових послуг, контрактування, взаємного визнання документів та участі громадян України в сервісній екосистемі внутрішнього ринку ЄС.

Ще один важливий кейс – роумінг. Після тимчасових домовленостей між операторами ЄС та України, які Єврокомісія підтримувала з 2022 року і продовжила 2024, 2025 року було ухвалено рішення про включення України до зони «Roam like at Home» з 1 січня 2026 року. На політичному рівні це перший випадок поширення внутрішньої політики ЄС на державу, що не є членом ЄС/ЄЕЗ, а на практичному рівні – це зниження бар'єрів для мільйонів громадян,

бізнесу та державних службовців, які переміщуються між Україною та ЄС. У безпековому сенсі це також елемент комунікаційної стійкості.

Водночас попри безсумнівні успіхи цифровізація в умовах війни має низку системних ризиків. По-перше, зберігається інфраструктурна вразливість: руйнування телекомунікацій, залежність від електропостачання, нерівномірність покриття та потреба в швидкому відновленні мереж. По-друге, існує ризик асиметрії між швидкістю запуску сервісів та якістю управління даними: зростання кількості сервісів потребує збалансованої архітектури реєстрів, захисту персональних даних, логування доступу та сумісності між відомчими системами.

По-третє, воєнна цифровізація загострює ризик центрування на «фронтенді», коли політична увага концентрується на видимих сервісах, тоді як менш помітні, але фундаментальні елементи – реєстрова чистота, бек-апи, стійкість муніципальних систем, кібергігієна місцевих органів, захист поштової інфраструктури – відстають. Матеріали CERT-UA за 2024-2025 роки свідчать, що саме місцеві органи влади, військовий сегмент, службові поштові скриньки та інтернет-доступні адміністративні інтерфейси стають одними з найуразливіших точок.

По-четверте, донорозалежність є одночасно перевагою і ризиком. Проєкти ЄС, UNDP, ITU та інших партнерів забезпечують масштабування сервісів, доступність, сумісність і модернізацію. Проте в довшій перспективі Україні потрібен перехід від моделі «проєктного підживлення» до стабільної бюджетної та інституційної моделі підтримки критичних цифрових систем, інакше післявоєнна фаза може виявити розрив між пілотами/грантами і сталою державною експлуатацією.

По-п’яте, зберігається питання інклюзивності. Цифрова держава ефективна лише тоді, коли не відтворює нові нерівності. Саме тому рішення про вебдоступність, підготовку державного стандарту доступності, інклюзивний дизайн сервісів та підтримку вразливих груп треба трактувати не як соціальну

«надбудову», а як безпековий стандарт публічного управління: недоступний сервіс у кризовій ситуації так само проблемний, як і нефункціональний [9].

Висновки. Цифровізація України в умовах війни є не просто продовженням довоєнної політики електронного урядування, а якісно новою фазою трансформації державного управління. Її центральний ефект полягає в тому, що цифрові технології стали механізмом реалізації основних функцій держави під умовами високої невизначеності: збереження керованості, підтримання сервісів, адміністрування соціальної допомоги, захисту даних, кризової комунікації та міжнародної координації. У цьому сенсі війна не скасувала цифрову реформу, а розкрила її справжню стратегічну цінність.

Аналітично доведено, що українська модель має щонайменше чотири сильні сторони. По-перше, вона змогла поєднати сервісну орієнтацію на громадянина з безпековою логікою резервування та неперервності. По-друге, вона побудована на законодавчих змінах, а не лише на адміністративних експериментах. По-третє, вона продемонструвала високу адаптивність у кіберпросторі, де відбиття атак супроводжувалося швидким інституційним навчанням. По-четверте, вона виявилася сумісною з європейською інтеграцією, перетворившись на один із найдинамічніших треків наближення до ЄС.

Водночас стратегічна стійкість цифрової держави залежатиме від того, чи зможе Україна подолати поточні обмеження: інфраструктурну вразливість телекоммереж, нерівномірну спроможність органів влади, ризики для поштових і локальних ІТ-контурів, залежність від зовнішнього проєктного фінансування та потребу глибшої гармонізації з правом ЄС. Найважливіший висновок полягає в тому, що дальша цифрова політика має бути сконструйована як політика державної стійкості. Відповідно, успіх повоєнної цифрової модернізації вимірюватиметься не лише кількістю сервісів, а здатністю держави надавати, захищати, відновлювати та транскордонно визнавати свої цифрові функції в екстремальних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OECD. *Digitalisation for recovery in Ukraine*. 2022. URL: https://www.oecd.org/en/publications/digitalisation-for-recovery-in-ukraine_c5477864-en.html.

2. Kolodii R. The pedagogy of Cyber-WAR : Explaining Ukraine's resilience against Russian cyber-aggression. *Defense & Security Analysis*. 2024. URL: https://www.tandfonline.com/toc/cdan20/40/2.

3. ITU. *Ukraine Digital Development Country Profile*. ITU activities related to Resolution 1408 on Ukraine. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf.

4. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18.09.2019 № 856; Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг : постанова Кабінету Міністрів України від 04.12.2019 № 1137. URL: https://zakon.rada.gov.ua/go/856-2019-%D0%BF/ed20191219.

5. Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX; Деякі питання надання та використання хмарних послуг та/або послуг центру обробки даних від 11.02.2025 № 154. URLhttps://zakon.rada.gov.ua/go/2075-20.

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19.

7. CERT-UA / Держспецзв'язку. Офіційні повідомлення та звіти про Industroyer2, хвилі деструктивного ПЗ, атаки Sandworm, Kyivstar, кампанії 2024–2025 років і огляд кіберзагроз 2025. URL: https://cip.gov.ua/en/news/poperedzhena-masshtabna-kiberataka-na-energetichnii-sektor-ukrayini.

8. E-Governance Academy. *DT4UA project*; *DT4UA project results*. URL: https://ega.ee/ega-supports-ukraines-digital-path-to-the-eu-dt4ua-project-results.

9. UNDP Ukraine. *Opinions and views of Ukrainians on state electronic services in 2024*. *DIA Support project*. URL:

https://www.undp.org/ukraine/publications/analytical-report-opinions-and-views-ukrainians-state-electronic-services-2024.

REFERENCES

1. OECD. *Digitalisation for recovery in Ukraine*. (2022). URL: https://www.oecd.org/en/publications/digitalisation-for-recovery-in-ukraine_c5477864-en.html. [in English]

2. Kolodii R. *The pedagogy of Cyber-WAR* : Explaining Ukraine's resilience against Russian cyber-aggression. (2024). *Defense & Security Analysis*. URL: https://www.tandfonline.com/toc/cdan20/40/2. [in English]

3. ITU. *Ukraine Digital Development Country Profile*. (2025). ITU activities related to Resolution 1408 on Ukraine. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf. [in English]

4. Pytannia Ministerstva tsyfrovoi transformatsii : postanova Kabinetu Ministriv Ukrainy vid 18.09.2019 № 856. (2019). [Issues of the Unified State Web Portal of Electronic Services and the Register of Administrative Services : Resolution of the Cabinet of Ministers of Ukraine dated 04.12.2019 No. 1137]. URL: https://zakon.rada.gov.ua/go/856-2019-%D0%BF/ed20191219. [in Ukrainian]

5. Pro khmarni posluhy : Zakon Ukrainy vid 17.02.2022 № 2075-IX. (2022). [Some issues of providing and using cloud services and/or data center services dated 11.02.2025 No. 154]. URL: https://zakon.rada.gov.ua/go/2075-20. [in Ukrainian]

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII. (2017). [For the basic principles of cyber security in Ukraine : Law of Ukraine dated 05.10.2017 No. 2163-VIII]. URL: https://zakon.rada.gov.ua/go/2163-19. [in Ukrainian]

7. CERT-UA (2025). [State Special Communications Service. Official announcements and reports on Industroyer2, waves of destructive software, Sandworm attacks, Kyivstar, 2024–2025 campaigns, and an overview of cyber threats]. URL:

https://cip.gov.ua/en/news/poperedzhena-masshtabna-kiberataka-na-energetichnii-sektor-ukrayini. [in Ukrainian]

8. E-Governance Academy. *DT4UA project*; *DT4UA project results*. URL: https://ega.ee/ega-supports-ukraines-digital-path-to-the-eu-dt4ua-project-results. [in English]

9. UNDP Ukraine. *Opinions and views of Ukrainians on state electronic services in 2024. DIA Support project*. URL: https://www.undp.org/ukraine/publications/analytical-report-opinions-and-views-ukrainians-state-electronic-services-2024. [in English]

Дата першого надходження статті до видання: 21.03.2026

Дата прийняття статті до друку після рецензування: 28.04.2026

Дата публікації (оприлюднення) статті: 29.05.2026