УДК 351:327

Гриненько Ігор Іванович
аспірант кафедри публічного управління та адміністрування
Івано-Франківського національного технічного університету нафти і газу
Hrynenko Ihor
PhD Student of the Department of Public Management and Administration
Ivano-Frankivsk National Technical University of Oil and Gas
ORCID: 0009-0008-2074-2147

DOI: 10.25313/2617-572X-2025-12-11745

ВИКЛИКИ ЦИФРОВІЗАЦІЇ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

CHALLENGES OF DIGITALIZATION OF LOCAL GOVERNMENT BODIES IN UKRAINE UNDER MARTIAL LAW

Анотація. *Мета. Метою дослідження є визначення, класифікація та системний аналіз ключових викликів цифровізації органів місцевого самоврядування (ОМС) в Україні в умовах правового режиму воєнного стану, а також обґрунтування концепції «кризової цифровізації» як механізму забезпечення інституційної стійкості територіальних громад.*

Методологія. У процесі дослідження використано комплекс загальнонаукових методів: системного аналізу – для вивчення цифровізації як цілісного процесу в системі публічного управління; порівняльного аналізу – для зіставлення рівнів цифрової зрілості громад у тилових та прифронтових регіонах; статистичного аналізу – для оцінки впливу воєнних дій на IT-сектор та енергетичну інфраструктуру; формально-юридичного методу – для характеристики нормативного забезпечення цифрового врядування в умовах надзвичайних правових режимів. Емпіричну базу дослідження склали дані 20 територіальних громад, які є репрезентативними для територій з населенням до 10 тис. осіб.

Результати. У статті здійснено комплексний аналіз трансформації цифрового врядування на місцевому рівні. Доведено, що повномасштабна війна суттєво трансформувала логіку цифрової трансформації, змістивши акцент із сервісної модернізації публічних послуг на забезпечення управлінської безперервності, кризового реагування та соціальної підтримки населення. На основі емпіричних даних виявлено значну асиметрію цифрової спроможності територіальних громад, зумовлену відмінностями фінансових, кадрових і технологічних ресурсів. Автором систематизовано основні групи викликів (інфраструктурні, кадрові, безпекові, фінансові), які стримують розвиток е-врядування в громадах під час війни.

Наукова новизна. Автором уперше розроблено класифікацію бар'єрів цифровізації ОМС воєнного часу та запропоновано введення в науковий обіг поняття «кризова цифровізація», що передбачає пріоритет функцій кібербезпеки, резервування даних та соціальної підтримки над класичними адміністративними сервісами.

Практичне значення. Одержані результати та розроблена класифікація викликів можуть бути використані для впровадження уніфікованого Паспорта цифрової стійкості громади, коригування місцевих програм інформатизації, формування політик безпеки даних та розробки стратегій відновлення громад.

Перспективи подальших досліджень. Подальшого вивчення потребують механізми інтеграції локальних цифрових систем із європейськими екосистемами (eIDAS) в контексті повоєнної відбудови та євроінтеграції України.

Ключові слова: *цифровізація, органи місцевого самоврядування, цифрове врядування, воєнний стан, публічне управління, кібербезпека, територіальні громади, кризова стійкість.*

Summary. *Purpose. The study aims to identify, classify, and systematically analyze the key challenges of digitalizing local self-government bodies (LSGBs) in Ukraine under the legal regime of martial law, as well as to substantiate the concept of "crisis digitalization" as a mechanism for ensuring the institutional resilience of territorial communities.*

Methodology. The study employs a complex of general scientific methods: systems analysis to study digitalization as a holistic process within the public administration system; comparative analysis to contrast levels of digital maturity in rear and frontline regions; statistical analysis to assess the impact of hostilities on the IT sector and energy infrastructure; and the formal-legal

method to characterize the regulatory framework of digital governance under emergency regimes. The empirical basis includes data from 20 territorial communities, representative of territories with a population of under 10,000 people.

Results. The article provides a comprehensive analysis of the transformation of digital governance at the local level. It is proven that the full-scale war has fundamentally altered the logic of digital transformation, shifting the focus from service-oriented modernization to ensuring managerial continuity, crisis response, and social support. Based on empirical data, a significant asymmetry in the digital capacity of territorial communities was revealed, driven by disparities in financial, human, and technological resources. The author systematizes the main groups of challenges (infrastructural, personnel, security, financial) hindering the development of e-governance during the war.

Scientific Novelty. For the first time, a classification of barriers to the digitalization of LSGBs in wartime is developed, and the concept of "crisis digitalization" is introduced into scientific circulation. This concept implies prioritizing cybersecurity, data backup, and social support functions over classical administrative services.

Practical Significance. The obtained results and the developed classification of challenges can be used for the implementation of a unified Digital Resilience Passport for the community, adjustment of local informatization programs, formulation of data security policies, and development of community recovery strategies.

Prospects for Further Research. Mechanisms for integrating local digital systems with European ecosystems (eIDAS) in the context of Ukraine's post-war reconstruction and European integration require further study.

Key words: *digitalization, local self-government bodies, digital governance, martial law, public administration, cybersecurity, territorial communities, crisis resilience.*

Постановка проблеми. Цифровізація органів місцевого самоврядування (ОМС) в Україні тривалий час розглядалася як послідовний еволюційний процес модернізації управлінських практик, спрямований на підвищення ефективності, прозорості та якості надання публічних послуг. Однак запровадження воєнного стану внаслідок повномасштабної збройної агресії суттєво змінило умови реалізації цифрової трансформації на локальному рівні, актуалізувавши низку системних суперечностей між стратегічними цілями цифрового розвитку та реальними управлінськими, ресурсними й безпековими обмеженнями діяльності територіальних громад.

Органи місцевого самоврядування в умовах війни змушені функціонувати в режимі постійної невизначеності, поєднуючи виконання розширених повноважень у сфері цивільного захисту, соціальної підтримки населення та відновлення критичної інфраструктури з необхідністю забезпечення безперервності управлінських процесів. За таких обставин цифрові інструменти управління набувають ознак критично важливої інфраструктури, водночас їх впровадження та використання супроводжуються інфраструктурними руйнуваннями, дефіцитом кваліфікованих кадрів, підвищеними кіберзагрозами та фрагментарністю нормативно-правового регулювання.

Проблемність ситуації полягає в тому, що наявні державні та місцеві стратегії цифрової трансформації здебільшого були сформовані для умов стабільного розвитку та не повною мірою враховують специфіку воєнного стану, асиметричність спроможності територіальних громад і необхідність інтеграції цифровізації з завданнями кризового управління та безпеки. Невирішеною частиною загальної проблеми є відсутність системного наукового осмислення класифікації ризиків цифровізації саме на муніципальному рівні, що обмежує здатність ОМС використовувати технології для забезпечення інституційної стійкості.

Аналіз останніх досліджень та публікацій. У сучасній українській науковій літературі значну увагу приділено проблематиці цифрових прав людини та трансформації механізмів їх реалізації. Зокрема, у працях Ю. С. Размєтаєвої [13] розкрито сутність цифрових прав і загрози їм у цифрову епоху. Вплив воєнного стану на доступ до цифрових сервісів відображено у дослідженнях І. С. Борка та О. М. Косова [14].

Проблеми цифровізації публічного управління та місцевого самоврядування розглядають Н. М. Піскоха та Г. О. Демошенко [15], а також автори колективної монографії за редакцією О. В. Карпенка [16], де цифрове врядування визначається як чинник стійкості управлінських систем. Водночас інші дослідники наголошують, що війна прискорила цифрову трансформацію як інструмент безпеки. Разом із тим, наявні дослідження потребують подальшого узагальнення саме в частині комплексного аналізу та класифікації викликів цифровізації ОМС.

Метою статті є визначення, класифікація та аналіз основних викликів цифровізації органів місцевого самоврядування в Україні в умовах воєнного стану.

Виклад основного матеріалу. Аналізуючи сучасні тенденції розвитку публічного управління на місцевому рівні, слід насамперед окреслити понятійно-категоріальний апарат дослідження. Відповідно до Закону України «Про місцеве самоврядування в Україні» [1], органи місцевого самоврядування є елементами публічної влади, через які територіальні громади реалізують гарантоване Конституцією право на самостійне вирішення питань місцевого значення.

Однією з найважливіших особливостей досліджуваного об'єкта є поступове ускладнення

функціонального навантаження органів місцевого самоврядування в умовах цифрової трансформації. Український курс на цифровізацію місцевого самоврядування формується у тісному взаємозв'язку з європейськими стратегічними орієнтирами (Програма «Цифрове десятиліття» ЄС до 2030 року) [2].

Нормативно-правова база цифровізації ОМС в Україні формується через низку спеціальних законодавчих актів: Закони України «Про електронну ідентифікацію та електронні довірчі послуги» [3], «Про електронні комунікації» [4], а також Закон «Про особливості надання публічних (електронних публічних) послуг» [5], який запровадив принцип «paperless».

У контексті цього дослідження пропонується ввести в науковий обіг поняття «кризова цифровізація» (crisis digitalization), визначивши її як специфічну модель управління цифровим розвитком в умовах екстремальних зовнішніх загроз, що характеризується докорінним зміщенням пріоритетів від сервісної орієнтованості (зручність, швидкість, клієнтоцентричність) до інституційної стійкості (кібербезпека, резервування даних, енергонезалежність). На відміну від класичної цифровізації, метою якої є оптимізація адміністративних процесів, метою кризової цифровізації є збереження керованості системою та фізичний захист цифрових активів громади.

Таким чином, запровадження правового режиму воєнного стану трансформувало пріоритети розвитку. Цифровізація ОМС фактично переходить у режим «кризової цифровізації», коли критерії ефективності доповнюються критеріями безпеки. За результатами аналізу емпіричних даних (дослідження Transparency International Ukraine, звіти ООН [6; 7]) автором виявлено суттєву асиметрію цифрового розвитку громад.

Для ілюстрації виявленої асиметрії проведено порівняльний аналіз пріоритетів цифровізації у двох типах громад: Львівська (тиловий регіон, захід України) та Херсонська (прифронтовий регіон, південь України).

Львівська громада. Ключовим вектором залишається «сервісна цифровізація». У 2023–2025 роках у бюджеті громади збережено видатки на оцифрування містобудівної документації та впровадження елементів Smart City (е-квиток, системи моніторингу повітря). Основний виклик — інтеграція внутрішньо переміщених осіб (ВПО) у цифрові реєстри громади та навантаження на ЦНАП. Фактично, тут зберігається класична парадигма New Public Management, де цифровізація є інструментом комфорту та інвестиційної привабливості.

Херсонська громада. Пріоритети зміщено виключно на «безпекову цифровізацію». Капітальні видатки на розвиток заблоковано. Зусилля ІТ-відділів зосереджені на: фізичній евакуації серверного обладнання, розгортанні мереж резервного зв'язку (Starlink) для об'єктів критичної інфраструктури та закритті публічного доступу до геопросторових даних. Порівняння показує, що в Херсонській громаді індекс цифрової зрілості тимчасово знизився через вимушену відмову від відкритих даних, тоді як Львівська громада продовжує нарощувати цифровий капітал. Це підтверджує тезу про формування «двошвидкісної» моделі цифровізації в Україні. Така ситуація створює ризик довгострокового «цифрового розриву», коли на заході країни впроваджуються європейські практики Good Governance (прозорість), а на півдні та сході закріплюється модель Crisis Governance (закритість заради виживання).

Для систематизації виявлених проблем та наукового обґрунтування необхідних управлінських рішень автором розроблено класифікацію викликів цифровізації, що дозволяє комплексно оцінити їхній вплив на діяльність ОМС (табл. 1).

Таблиця 1

Класифікація викликів цифровізації органів місцевого самоврядування в умовах воєнного стану

Група викликів	Зміст виклику (прояв)	Наслідки для ОМС
Інфраструктурні	Руйнування енергетичних об'єктів, нестабільність інтернет-зв'язку, пошкодження телекомунікаційних мереж.	Перебої в наданні е-послуг, необхідність переходу на «паперові» резерви, витрати на альтернативні джерела живлення.
Безпекові (Кібернетичні)	DDoS-атаки на вебпортали громад, фішинг, злам акаунтів у соцмережах, спроби несанкціонованого доступу до реєстрів.	Витік персональних даних мешканців, дезінформація населення, блокування роботи місцевих рад.
Кадрові	Мобілізація ІТ-фахівців, відтік кваліфікованих кадрів за кордон, психологічне вигорання персоналу.	Дефіцит компетенцій для підтримки цифрових систем, неможливість впровадження складних проєктів.
Фінансові	Секвестр місцевих бюджетів, пріоритет видатків на оборону, обмеження капітальних видатків (постанова КМУ № 590 [17]).	Відсутність коштів на модернізацію обладнання, закупівлю ліцензійного ПЗ та сучасних систем захисту інформації.
Управлінські	Асиметрія розвитку громад, відсутність єдиних стандартів «кризової цифровізації», фрагментарність рішень.	Поглиблення «цифрового розриву» між громадами, дублювання функцій, низька інтероперабельність локальних систем.

Джерело: власна розробка автора

Аналіз, наведений у табл. 1, свідчить, що функціонування цифрових сервісів ОМС критично залежить від енергетичної стабільності. Як зазначають аналітики, втрати енергетичних об'єктів призвели до зниження генеруючої потужності, що змусило громади інвестувати в резервне живлення [9].

Крім того, цифровізація в умовах війни неминуче супроводжується зростанням кіберризиків. Як свідчать дані Держспецзв'язку та міжнародних звітів [11; 12], локальний рівень управління залишається одним із найбільш уразливих елементів національної системи кібербезпеки. Бюджетні обмеження не дозволяють більшості громад побудувати ешелонований захист, що потребує втручання на державному рівні.

В умовах дії Постанови КМУ № 590, яка обмежує капітальні видатки з місцевих бюджетів (зокрема на закупівлю коштовного серверного обладнання), основним джерелом фінансування кіберстійкості стає міжнародна технічна допомога (МТД). Варто зазначити, що саме Постанова № 590 створює інституційну пастку: громади мають обов'язок захищати дані (згідно із Законом про захист інформації), але не мають права закуповувати для цього сервери (CAPEX). Виходом із цієї ситуації є перехід до моделі операційних витрат (OPEX) через оренду хмарних сховищ (IaaS/SaaS), що дозволено Законом України «Про хмарні послуги» [18] і не підпадає під жорсткі обмеження казначейства.

Аналіз успішних кейсів 2023–2025 років демонструє ефективність співпраці громад з донорськими програмами:

1. Програма «U-LEAD з Європою»: надає консультаційну підтримку та обладнання для відновлення цифрових послуг на деокупованих територіях.

2. Проєкти USAID (зокрема HOVERLA): забезпечували громади засобами супутникового зв'язку та генераторами для підтримки безперервності роботи ІТ-інфраструктури.

3. Гранти в рамках програми ЄС «Цифрова Європа» (Digital Europe Programme): дозволяють українським муніципалітетам подаватися на фінансування проєктів з кібербезпеки спільно з європейськими партнерами.

Отже, ОМС рекомендується переорієнтувати роботу відділів економічного розвитку на написання грантових заявок саме під компоненти «цифрової

Таблиця 2

Типова структура Паспорта цифрової стійкості територіальної громади

Структурний блок	Зміст та ключові компоненти	Відповідальний за реалізацію
1. Адміністративно-правовий статус	• Рівень затвердження: рішення виконавчого комітету або розпорядження начальника військової адміністрації (без винесення на сесію ради). • Гриф доступу: «Для службового користування» (ДСК). • Періодичність оновлення: щоквартально або невідкладно при зміні безпекової ситуації.	Керуючий справами виконкому / секретар ради
2. Протокол інфраструктурного резервування	• Енергонезалежність: перелік критичного обладнання (сервери, комутатори) із закріпленими джерелами живлення (генератори, UPS) та розрахунком часу автономної роботи. • Резервний зв'язок: схема розгортання терміналів супутникового зв'язку (Starlink) та альтернативних каналів Інтернет (оптоволокно/радіоканал).	Начальник відділу господарського забезпечення / ІТ-адміністратор
3. Протокол безпеки даних (Data Protocol)	• Резервне копіювання: графік створення бекапів (наприклад: бази даних — щоденно, файлові архіви — щотижнево). • Локація зберігання: хмарні сховища (у межах виконання принципу OPEX замість CAPEX) або сервери в захищених дата-центрах на безпечних територіях. • Контроль доступу: реєстр працівників із правами доступу до реєстрів та графік зміни паролів/ключів.	Системний адміністратор / адміністратор безпеки
4. Протокол «Цифрової евакуації»	• Алгоритм дій (Trigger points): чіткий перелік умов для активації (наприклад, наближення лінії фронту на 20 км). • Фізичне знищення: інструкція зі знищення апаратних ключів КЕП (токенів) та жорстких дисків, які неможливо евакуювати. • Блокування: процедура екстреного відключення користувачів від державних реєстрів та видалення облікових записів.	Голова громади / начальник ВА (особистий контроль)
5. Кадрова взаємозамінність	• Матриця компетенцій: перелік дублерів для критичних ролей (хто адмініструє систему, якщо основний ІТ-фахівець мобілізований або евакуйований). • Контакти підтримки: прямі контакти регіональних координаторів Мінцифри та кіберполіції.	Керівник відділу кадрів

Джерело: власна розробка автора

безпеки», що наразі є пріоритетом для міжнародних донорів.

Кадровий аспект також є критичним. Попри державні програми перекваліфікації («IT Generation» тощо), ефективність інтеграції нових кадрів в публічний сектор залишається низькою через неконкурентні заробітні плати в ОМС порівняно з приватним сектором [10]. Заробітна плата ІТ-спеціаліста в органах місцевого самоврядування регламентована тарифною сіткою і є у 5–7 разів нижчою за ринкову. Аналіз штатних розписів 20 територіальних громад показав, що функції адміністратора безпеки та системного адміністратора у 85% випадків виконують непрофільні працівники (землевпорядники, діловоди) як додаткове навантаження. Це створює прямі вразливості для національної системи кібербезпеки, адже саме через слабко захищені комп'ютери в громадах хакери часто отримують доступ до центральних державних реєстрів.

У перспективі післявоєнного відновлення цифровізація ОМС має розглядатися як інституційний компонент стійкості громади. Для цього пропонується впровадження уніфікованого «Паспорта цифрової стійкості територіальної громади». Цей документ має містити не декларації, а чіткі інструкції:

1. Протокол інфраструктурного резервування (схеми підключення Starlink та генераторів).

2. Протокол даних (регулярність бекапів у захищені хмарні сховища).

3. Протокол цифрової евакуації (алгоритм фізичного знищення ключів КЕП та міграції реєстрів у разі загрози окупації).

Легітимізація такого документа має відбуватися не через публічні рішення сесій рад (що створює розвідувальні ризики), а через рішення виконавчих комітетів або розпорядження начальників військових адміністрацій з грифом «Для службового користування», що убезпечить чутливу інформацію від ворога. Наявність такого Паспорта має перевірятися регіональними координаторами з цифровізації (CDTO) при обласних військових адміністраціях.

Для практичної реалізації зазначених принципів автором розроблено типову структуру Паспорта цифрової стійкості, яка може бути адаптована під потреби конкретної громади (табл. 2).

Основними завданнями залишаються: формування мінімальних стандартів цифрової інфраструктури, кадрове посилення та впровадження локальних політик кібербезпеки.

Висновки. Узагальнення результатів проведеного аналізу дозволяє дійти висновку, що цифровізація органів місцевого самоврядування в Україні в умовах воєнного стану набула характеру кризово-адаптивної трансформації.

Запропонована автором класифікація викликів (табл. 1) дозволяє чітко ідентифікувати слабкі місця в системі муніципального управління. З'ясовано, що найбільш критичними є інфраструктурні та безпекові загрози, які вимагають перегляду підходів до фінансування та технічного забезпечення громад.

Конкретні наукові пропозиції автора полягають у необхідності запровадження уніфікованого «Паспорта цифрової стійкості територіальної громади». Цей документ має містити інвентаризацію критичних ІТ-активів, схеми резервного живлення/зв'язку та протоколи дій у разі кібератак.

Механізм легітимізації. З огляду на безпековий характер документа, його затвердження має здійснюватися не рішенням сесії ради (що передбачає публічність), а рішенням виконавчого комітету з грифом «Для службового користування». У громадах, де введено військові адміністрації населених пунктів, паспорт затверджується розпорядженням начальника військової адміністрації. Такий підхід забезпечить оперативність прийняття рішень та захист чутливої інформації від ворога.

Перспективи подальших наукових досліджень пов'язані з вивченням механізмів міжмуніципальної кооперації та державно-приватного партнерства у сфері цифрових послуг як способу подолання асиметрії цифрового розвитку громад.

Література

1. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 р. № 280/97-ВР. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр (дата звернення: 10.12.2025).

2. Рішення (ЄС) 2022/2481 Європейського Парламенту та Ради від 14 грудня 2022 року про створення Програми політики «Цифрове десятиліття» до 2030 року. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32022D2481 (дата звернення: 12.12.2025).

3. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 10.12.2025).

4. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1089–20 (дата звернення: 10.12.2025).

5. Про особливості надання публічних (електронних публічних) послуг : Закон України від 15.07.2021 р. № 1689-IX. URL: https://zakon.rada.gov.ua/laws/show/1689-20 (дата звернення: 11.12.2025).

6. Опитування ООН щодо електронного урядування 2024 року. *Організація Об'єднаних Націй*. URL: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine (дата звернення: 15.12.2025).

7. Не «Дією» єдиною: які е-послуги надають українські міста. *Transparency International Ukraine*. 2022. URL: https://ti-ukraine.org/blogs/ne-diyeyu-yedynoyu-yaki-e-poslugy-nadayut-ukrayinski-mista/ (дата звернення: 05.12.2025).

8. Україна запускає новий електронний сервіс для внутрішньо переміщених осіб. *UNDP Ukraine*. URL: https://www.undp.org/uk/ukraine/press-releases/ukrayina-zapuskaye-novyy-elektronnyy-servis-dlya-vnutrishno-peremishchenykh-osib (дата звернення: 10.12.2025).

9. Уряд ухвалив 4 рішення для покращення ситуації з електропостачанням. *Прикарпаттяобленерго*. URL: https://oe.if.ua/uk/articles/69392fbced67d430329ec64a (дата звернення: 15.12.2025).

10. Цифрова трансформація під тиском обставин. *VoxUkraine*. URL: https://voxukraine.org/tsyfrova-transformatsiya-pid-tyskom-obstavyn (дата звернення: 18.12.2025).

11. Fyshchuk I. Stronger Together? EU Support for Ukrainian Local Authorities Facing Cyber Attacks (2022–2023). *ACIG Journal*. URL: https://www.acigjournal.com/pdf-190344-112707?filename=Stronger%20together_%20EU.pdf (дата звернення: 20.12.2025).

12. Bridging the cyber security gap: Why Ukrainian local authorities need more support for cyber security from the EU. *Hromada Network*. URL: https://hromada.network/ukrainian-hromadas-need-eu-cybersecurity-support/ (дата звернення: 20.12.2025).

13. Размєтаєва Ю. С. Права людини в епоху цифрових трансформацій: монографія. Харків: Право, 2022. 248 с.

14. Борко І. С., Косов О. М. Правове регулювання цифрової трансформації в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2023. № 2. С. 34–38. URL: http://www.lsej.org.ua/2_2023/8.pdf (дата звернення: 15.12.2025).

15. Піскоха Н. М., Демошенко Г. О. Цифровізація публічного управління як фактор сталого розвитку регіонів. *Публічне управління та митне адміністрування*. 2022. № 3 (34). С. 67–72.

16. Цифрове врядування : монографія / за ред. О. В. Карпенка. Київ : Ідея Принт, 2020. 336 с.

17. Про затвердження Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах воєнного стану : Постанова Кабінету Міністрів України від 09.06.2021 р. № 590. Офіційний вісник України. 2021. № 49. Ст. 3033. URL: https://zakon.rada.gov.ua/laws/show/590-2021-п (дата звернення: 11.12.2025)

18. Про хмарні послуги : Закон України від 17.02.2022 р. № 2075-IX. *Відомості Верховної Ради України*. 2023. № 5. Ст. 14. URL: https://zakon.rada.gov.ua/laws/show/2075-20 (дата звернення: 11.12.2025)

References

1. Verkhovna Rada of Ukraine. (1997). Pro mistseve samovriaduvannia v Ukraini [On Local Self-Government in Ukraine] (Law No. 280/97-VR). Ofitsiinyi vebportal Parlamentu Ukrainy. https://zakon.rada.gov.ua/laws/show/280/97-вр [in Ukrainian].

2. European Parliament and Council. (2022). Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022D2481.

3. Verkhovna Rada of Ukraine. (2017). Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [On Electronic Identification and Electronic Trust Services] (Law No. 2155-VIII). https://zakon.rada.gov.ua/laws/show/2155-19 [in Ukrainian].

4. Verkhovna Rada of Ukraine. (2020). Pro elektronni komunikatsii [On Electronic Communications] (Law No. 1089-IX). https://zakon.rada.gov.ua/laws/show/1089-20 [in Ukrainian].

5. Verkhovna Rada of Ukraine. (2021). Pro osoblyvosti nadannia publichnykh (elektronnykh publichnykh) posluh [On Peculiarities of Providing Public (Electronic Public) Services] (Law No. 1689-IX). https://zakon.rada.gov.ua/laws/show/1689-20 [in Ukrainian].

6. United Nations. (2024). United Nations E-Government Survey 2024: Ukraine country profile. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine.

7. Transparency International Ukraine. (2022). Ne "Diieiu" yedynoiu: yaki e-posluhy nadaiut ukrainski mista [Not by "Diia" alone: what e-services are provided by Ukrainian cities]. https://ti-ukraine.org/blogs/ne-diyeyu-yedynoyu-yaki-e-poslugy-nadayut-ukrayinski-mista/ [in Ukrainian].

8. United Nations Development Programme. (2022). Ukraina zapuskaie novyi elektronnyi servis dlia vnutrishno peremishchenykh osib [Ukraine launches a new electronic service for internally displaced persons]. https://www.undp.org/uk/ukraine/press-releases/ukrayina-zapuskaye-novyy-elektronnyy-servis-dlya-vnutrishno-peremishchenykh-osib [in Ukrainian].

9. Prykarpattiaoblenerho. (2023). Uriad ukhvalyv chotyry rishennia dlia pokrashchennia sytuatsii z elektropostachanniam [The government adopted 4 decisions to improve the electricity supply situation]. https://oe.if.ua/uk/articles/69392fbced67d430329ec64a [in Ukrainian].

10. VoxUkraine. (2024). Tsyfrova transformatsiia pid tyskom obstavyn [Digital transformation under pressure of circumstances]. https://voxukraine.org/tsyfrova-transformatsiya-pid-tyskom-obstavyn [in Ukrainian].

11. Fyshchuk, I. (2023). Stronger Together? EU Support for Ukrainian Local Authorities Facing Cyber Attacks (2022–2023). ACIG Journal. https://www.acigjournal.com/pdf-190344–112707?filename=Stronger%20together_%20EU.pdf.

12. Hromada Network. (2023). Bridging the cybersecurity gap: Why Ukrainian local authorities need more support for cyber security from the EU. https://hromada.network/ukrainian-hromadas-need-eu-cybersecurity-support/.

13. Razmietaieva, Yu. S. (2022). Prava liudyny v epokhu tsyfrovykh transformatsii [Human rights in the era of digital transformations]. Kharkiv: Pravo [in Ukrainian].

14. Borko, I. S., & Kosov, O. M. (2023). Pravove rehuliuvannia tsyfrovoi transformatsii v umovakh voiennoho stanu [Legal regulation of digital transformation under martial law]. Yurydychnyi naukovyi elektronnyi zhurnal, 2, 34–38. http://www.lsej.org.ua/2_2023/8.pdf [in Ukrainian].

15. Piskokha, N. M., & Demoshenko, H. O. (2022). Tsyfrovizatsiia publichnoho upravlinnia yak faktor staloho rozvytku rehioniv [Digitalization of public administration as a factor of sustainable development of regions]. Publichne upravlinnia ta mytne administruvannia, 3(34), 67–72 [in Ukrainian].

16. Karpenko, O. V. (Ed.). (2020). Tsyfrove vriaduvannia [Digital governance]. Kyiv: Ideia Prynt [in Ukrainian].

17. Cabinet of Ministers of Ukraine. (2021). Pro zatverdzhennia Poriadku vykonannia povnovazhen Derzhavnoiu kaznacheiskoiu sluzhboiu v osoblyvomu rezhymi v umovakh voiennoho stanu [On approval of the Procedure for exercising powers by the State Treasury Service under a special regime under martial law] (Resolution No. 590). https://zakon.rada.gov.ua/laws/show/590-2021-п [in Ukrainian].

18. Verkhovna Rada of Ukraine. (2022). Pro khmarni posluhy [On Cloud Services] (Law No. 2075-IX). https://zakon.rada.gov.ua/laws/show/2075-20 [in Ukrainian].

Стаття надійшла до редакції 29.12.2025