УДК 35:004:351.86(477)

І. М. Перестюк,
к. держ. упр., доцент,
доцент кафедри національної безпеки та підприємництва, Державне некомерційне підприємство Державний університет "Київський авіаційний інститут"
ORCID ID: https://orcid.org/0000-0003-1692-9247
Г. П. Нестеренко,
к. держ. упр., доцент,
доцент кафедри національної безпеки та підприємництва, Державне некомерційне підприємство Державний університет "Київський авіаційний інститут"
ORCID ID: https://orcid.org/0000-0002-1106-3790

DOI: 10.32702/2306-6814.2026.6.369

ЦИФРОВІЗАЦІЇ ПУБЛІЧНИХ ПОСЛУГ В УКРАЇНІ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ: БЕЗПЕКОВИЙ АСПЕКТ

I. Perestiuk,
PhD in Public Administration, Associate Professor,
Associate Professor of the Department of National Security and Enterprise,
State Non-Profit Enterprise, State University "Kyiv Aviation Institute"
H. Nesterenko,
PhD in Public Administration, Associate Professor,
Associate Professor of the Department of National Security and Enterprise,
State Non-Profit Enterprise, State University "Kyiv Aviation Institute"

DIGITALIZATION OF PUBLIC SERVICES IN UKRAINE UNDER MARTIAL LAW: THE SECURITY ASPECT

У статті здійснено комплексний науковий аналіз цифровізації публічних послуг в Україні в умовах воєнного стану як складової трансформації системи публічного управління та елементу національної стійкості. Визначено, що в період повномасштабної війни цифровізація набуває безпекового та стійкісного змісту, трансформуючись із інструменту адміністративної модернізації у механізм забезпечення безперервності реалізації державних функцій, кризового реагування та інституційної стабільності. Проаналізовано наукові підходи до цифрової трансформації публічного управління, інституційні засади розвитку цифрової держави, а також міжнародні оцінки функціонування українських цифрових платформ. Окремо проаналізовано значення Системи електронної взаємодії органів публічної влади як ключового елементу міжвідомчої інтеграції та управлінської стійкості. Обгрунтовано необхідність переорієнтації стратегічних орієнтирів цифровізації з кількісного розширення сервісів на забезпечення їх безперервності, кіберзахищеності та інтегрованості в умовах дії воєнного стану. Узагальнено інституційні, технологічні та соціально-компетентнісні виклики цифровізації, серед яких фрагментарність регуляторного поля, нечіткість розподілу відповідальності за цифрові сервіси, кіберзагрози та гібридні атаки, залежність від енергетичної інфраструктури, обмежена резервованість систем, цифрова нерівність населення та дефіцит цифрових і кіберкомпетентностей публічних служ-

бовців. Систематизовано стратегічні напрями удосконалення цифровізації публічних послуг, що охоплюють інституційну стандартизацію цифрової екосистеми, впровадження моделі управління цифровими ризиками, посилення кіберстійкості державних інформаційних ресурсів, розвиток гібридної моделі надання послуг, формування компетентнісного потенціалу персоналу та інтеграцію цифровізації у систему національної безпеки. Зроблено висновок, що в умовах воєнного стану цифрові публічні послуги виконують функцію інфраструктури державної стійкості, а їх розвиток має грунтуватися на інтеграції сервісності, безпеки та управлінської адаптивності.

The article provides a comprehensive scientific analysis of the digitalization of public services in Ukraine under martial law as a component of the transformation of the public administration system and an element of national resilience. It is determined that during the period of full-scale war, digitalization acquires a security— and resilience-oriented dimension, transforming from an instrument of administrative modernization into a mechanism for ensuring the continuity of public functions, crisis response, and institutional stability. The study analyzes scholarly approaches to the digital transformation of public administration, the institutional foundations of digital state development, as well as international assessments of the functioning of Ukrainian digital platforms. Particular attention is devoted to the Electronic Interaction System of Executive Authorities as a key element of interagency integration and managerial resilience. The necessity of reorienting strategic priorities of digitalization from the quantitative expansion of services toward ensuring their continuity, cybersecurity, and systemic integration under wartime risks is substantiated. Institutional, technological, and socio-competence-related challenges of digitalization are generalized, including the fragmentation of the regulatory framework, the lack of clear allocation of responsibility for digital services, cyber threats and hybrid attacks, dependence on energy infrastructure, limited system redundancy, digital inequality among citizens, and the shortage of digital and cybersecurity competencies among public servants. Strategic directions for improving the digitalization of public services are systematized, encompassing institutional standardization of the digital ecosystem, the implementation of a digital risk management model, strengthening the cybersecurity resilience of public information resources, the development of a hybrid service delivery model, enhancement of personnel competencies, and the integration of digitalization into the national security system. It is concluded that under martial law, digital public services function as an infrastructure of state resilience, and their further development should be based on the integration of service orientation, security, and managerial adaptability.

Ключові слова: публічна політика, цифровізація публічних послуг, цифрові компетентності, кібербезпека, інтероперабельність, система електронної взаємодії органів публічної влади, цифрові ризики, цифрові платформи на публічній службі, національна безпека, воєнний стан, комунікації органів публічної влади.

Key words: public policy, digitalization of public services, digital competencies, cybersecurity, interoperability, electronic interaction system of public authorities, digital risks, digital platforms in public service, national security, martial law, communications of public authorities.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Цифровізація в публічному управлінні в Україні набула системного характеру та перетворилася на один із ключових напрямів трансформації держави, особливо в умовах воєнного стану. Інституціоналізація цифрових рішень, впровадження цифрових платформ на державній службі, розбудова системи електронної взаємодії органів публічної влади та реалізація Концепції розвитку цифрової держави формують нову модель надання публічних послуг. Водночас воєнні ризики, нерівномірність цифрової інфраструктури, дефіцит цифрових компетентностей публічних службовців і фрагментарність міжвідомчої інтеграції зумовлюють появу системних викликів.

Особливої актуальності набуває проблема узгодження стратегічних орієнтирів цифрової трансформації з потребами національної безпеки, забезпеченням міжвідомчої електронної взаємодії та формуванням належного рівня цифрових компетентностей у системі публічної служби. Таким чином, постає необхідність комплексного наукового осмислення інституційних, організаційних та безпекових аспектів цифровізації публічних послуг в Україні в умовах воєнного стану.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Ю. Завгородня (2025) [2] акцентує на трансформації політики цифровізації органів місцевого самоврядування під впливом воєнних ризиків. В. Кучменко та М. Ватульєв (2025) [3] розглядають цифрову трансформацію як складову кризового управління та національної стійкості. І. Лопушинський, В. Клюцевський та О. Момоток (2023) [4] підкреслюють роль електронних сервісів у забезпеченні безперервності державних функцій в умовах обмеженої доступності традиційних каналів. Т. Малахова (2025) [5] обгрунтовує необхідність інституційних і технологічних механізмів захисту державних інформаційних ресурсів. Нормативну основу цифрової трансформації формує розпорядження Кабінету Міністрів України № 67-р (2018) [6]. І. Скляр (2024) [7] звертає увагу на регресивні прояви та обмеження цифрового врядування під впливом воєнних факторів. Ю. Шпак, А. Кожина та І. Драган (2025) [8] досліджують проблеми стандартизації та інтероперабельності цифрових рішень.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є дослідження цифровізації публічних послуг в Україні, аналіз викликів та загроз з урахуванням безпекового аспекту цифровізації публічного управління в період дії воєнного стану.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

І. Лопушинський, В. Ключевський та О. Момоток наголошують, що цифрові сервіси, включно із мобільними платформами, стають інструментом безперервності державних функцій і підтримки громадян за обмеженої доступності традиційних каналів [4]. Ми погоджуємося із твердженням авторів, але уточнюємо, що безперервність виникає лише за наявності стійкої інфраструктури, кіберзахисту, узгодженої міжвідомчої взаємодії, а також достатніх цифрових компетентностей персоналу. Показовими є висновки І. Скляра, який, аналізуючи розвиток цифрового врядування під час повномасштабної війни, звертає увагу на наявність обмежень і регресивних проявів унаслідок воєнних факторів та режимних обмежень [7]. Воєнний контекст оголює прогалини цифрового публічного управління: залежність від інфраструктури, чутливість реєстрів і даних, асиметрію доступу населення до цифрових каналів.

Базовим орієнтиром цифровізації в Україні є розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018—2020 роки та затвердження плану заходів щодо її реалізації" від 17 січня 2018 року № 67-р, яке закладає стратегічні пріоритети цифрової модернізації та план заходів [6]. Концепція задає напрям "державних сервісів онлайн", але її положення потребують переосмислення крізь призму ризиків воєнного часу. В. Кучменко та М. Ватульєв фіксують, що в умовах воєнного стану цифрова трансформація набуває безпекового та стійкісного змісту, адже цифрові сервіси стають частиною національної стійкості та кризового реагування [3]. Ми погоджуємося з позицією і пропонуємо її операціоналізацію модернізація публічного управління через цифровізацію публічних послуг у воєнний час має оцінюватися за трьома критеріями:

— спроможність підтримувати критичні сервіси за руйнувань і переміщень;

— захищеність даних і каналів взаємодії від кібервпливів, кіберзагроз та кібератак;

— інтегрованість (система електронної взаємодії органів виконавчої влади та узгодженість реєстрів/процесів).

Водночас зауважимо, що ефективність системи електронної взаємодії органів виконавчої влади (далі СЕВ ОВВ) безпосередньо залежить від рівня стандартизації цифрових процесів, узгодженості форматів даних, надійності каналів зв'язку та кіберзахищеності інформаційних ресурсів. В умовах воєнного стану фрагментація інформаційних систем, нерівномірна технічна спроможність органів виконавчої влади та ризики кібератак можуть знижувати інтеграційний потенціал системи та створювати додаткові операційні ризики. Таким чином, СЕВ ОВВ виступає не лише технічним інструментом електронної комунікації, а ключовим елементом інституційної стійкості публічного управління, що потребує постійного удосконалення з урахуванням вимог безперервності, безпеки та інтегрованості управлінських процесів.

Міжнародний науковий дискурс підтверджує релевантність такого підходу. Дослідження про адаптивне врядування під час війни підкреслює роль державних цифрових платформ у підтриманні доступу до послуг навіть за пошкодженої інфраструктури, а також значення координації (держави, місцевого самоврядування, громадянського суспільства) для швидких сервісних рішень [9]. Це важливо для українського контексту, оскільки цифрова трансформація відзначається керованою взаємодією інституцій, здатною працювати в умовах високої невизначеності. Таким чином, цифровізацію публічних послуг у воєнний час доцільно тлумачити як комплекс "сервіс + стійкість + безпека", де нормативно-стратегічні орієнтири формують вектор цифрової держави із врахуванням забезпечення безпеки даних.

Варто зазначити, що у воєнний період цифрові платформи в Україні виконують функцію інституційної стійкості, забезпечуючи швидкий доступ до послуг, зменшуючи потребу у фізичній присутності громадян та підтримуючи керованість публічних процесів за умов переміщення населення, ризиків для інфраструктури та кадрових втрат. До основних державних цифрових платформ доцільно віднести:

— екосистему "Дія": фронт-офіс цифрових послуг;

— "Трембіту": міжвідомча інтероперабельна інфраструктура обміну даними;

— інструменти е-ідентифікації, е-підпису та електронний документообіг у державних органах;

— мережу ЦНАП/Дія Центрів: фізичний контур безперервності послуг;

— Резерв+ та Оберіг: цифрові інструменти обліку призовників, військовозобов'язаних і резервістів;

— державні електронні реєстри та інформаційні системи (такі як державний демографічний реєстр, реєстри нерухомості, бізнесу, податкові та соціальні реєстри та ін.): базові джерела даних для надання публічних послуг та прийняття управлінських рішень.

Міжнародна оцінка SIGMA/OECD фіксує, що Україна суттєво посилила спроможності у сфері найсильніших компонентів публічного адміністрування, а динаміка використання ресурсів "Трембіти" у 2021—2025 роках є показовою навіть із провалами напочатку повномасштабної війни. Аналізуючи дані про роботу системи електронної взаємодії державних електронних інформаційних ресурсів Трембіта на основі звіту проекту EU4DigitalUA, зазначимо, що цифрові транзакції з моменту запуску системи Трембіта у 2020 році до 1 жовтня 2025 року склали 18,1 млрд, лише у 3-му кварталі 2025 року показник транзакцій був рекордний і склав — 3,4 млрд. При цьому "Трембіта" забезпечує захищену міжвідомчу взаємодію та охоплює 290 учасників, 1044 активні інформаційні взаємодії, будуючи взаємодії між реєстрами та інформаційними системами [10-12].

Окремо важливим є кадровий вимір цифрових платформ. О.-С. Бачинський обгрунтовує, що цифрові платформи у публічному управлінні посилюють комунікацію, автоматизацію кадрових процесів, доступ до навчальних ресурсів і моніторинг компетентностей. Водночас автор прямо вказує на бар'єри, зокрема, нерівномірність цифрової грамотності, регуляторну фрагментарність і невирішеність питань кібербезпеки [1]. Ми погоджуємося, але уточнюємо, що в умовах воєнного стану цифрові платформи є організаційним каркасом безперервності послуг, де кадрова адаптація є похідною від здатності системи зберегти процеси (дані → рішення → послуга).

Найсуттєвіші ризики державних цифрових платформ під час війни доцільно групувати у три блоки:

— ризики інтероперабельності та фрагментації систем: Ю. Шпак, А. Кожина та І. Драган підкреслюють, що за відсутності належної стандартизації цифрових рішень виникають проблеми несумісності інформаційних систем, розрізненості платформ і падіння керованості цифрової екосистеми [8];

— кібербезпекові ризики та ризики доступності: з огляду на стабільні атаки на державні інформаційні системи, саме кіберстійкість, резервування, сегментація доступів і безпечна інтеграція реєстрів стають умовою надання послуг;

— кадрові та компетентнісні ризики: О. Бачинський, Ю. Шпак, А. Кожина та Ю. Драган у різних площинах вказують на проблему цифрових компетентностей і нормативної узгодженості як фактори, що стримують ефективність цифровізації [1; 8]. У воєнний період цифрові компетентності мають оцінюватися, як здатність діяти за стандартами інформаційної безпеки, безперервності процесів, цифрової етики та захисту персональних даних, що напряму пов'язано з якістю публічних послуг і довірою до держави.

Таким чином, цифрові платформи в умовах воєнного стану виконують роль інфраструктури безперервності публічних послуг. Водночас ключові загрози концентруються у площині стандартизації та сумісності, кіберстійкості й компетентнісної спроможності персоналу, що вимагає цілісної управлінської логіки як основи цифровізації публічних послуг у період дії воєнного стану та в умовах забезпечення національної безпеки.

Наукові праці 2025 року деталізують загрози для органів публічної влади. Так, Т. Малахова розглядає кібербезпеку публічного управління крізь призму гібридних загроз, підкреслюючи потребу інституційних і технологічних механізмів протидії [5]. Додамо, що для публічних послуг ключовим стає розмежування відповідальності між власниками реєстрів/сервісів, адміністраторами та користувачами, а також процедурна готовність (плани реагування, резервування, відновлення сервісів).

Принагідно підкреслити, що цифрові публічні послуги залежать від фізичної інфраструктури. На рівні секторальних досліджень цифровізації місцевого самоврядування в період війни Ю. Завгородня прямо зазначає, що руйнування інфраструктури, обмеження доступу до офлайн-послуг і кіберзагрози формують специфічний контур цифрової нерівності та обмежують сталу доступність послуг [2]. Погоджуємося, оскільки інфраструктурні втрати посилюють потребу в гібридній моделі та пріоритизації "критичних послуг" у планах безперервності та забезпечення безпеки даних.

Доцільно структурувати виклики та загрози цифровізації публічних послуг в умовах воєнного стану. Така систематизація відображає характер та вплив загроз на стійкість, безперервність та якість надання публічних послуг.

Таблиця 1. Виклики та загрози цифровізації публічних послуг в умовах воєнного стану

Виклики	Прояви	Управлінський вимір ризику	Потенційні наслідки для публічних послуг
Інституційні виклики	фрагментарність регуляторного поля	невизначеність процедур цифрової взаємодії	дублювання функцій
	нечіткість розподілу відповідальності за цифрові сервіси	розмитість повноважень	підвищення операційних ризиків
	відсутність єдиної системи пріоритизації критичних послуг	нерівномірний розподіл ресурсів	уразливість стратегічно важливих сервісів
Технологічні загрози	кіберзагрози та гібридні атаки	порушення цілісності та конфіденційності даних	зупинка сервісів, витік інформації, зниження довіри
	залежність від енергетичної інфраструктури	неможливість стабільного функціонування платформ	тимчасова або повна недоступність послуг
	обмежена резервованість систем	відсутність альтернативних каналів функціонування	тривале відновлення після збоїв
Соціально-компетентнісні ризики	цифрова нерівність громадян	обмежений доступ окремих груп населення до онлайн-послуг	посилення соціальної диференціації
	дефіцит цифрових і кіберкомпетентностей публічних службовців	низька якість адміністрування цифрових процесів	підвищення помилок і операційних збоїв
	зниження довіри у випадку збоїв сервісів	репутаційні ризики державних інституцій	делегітимація цифрових реформ

Джерело: розробка авторів.

Таблиця 2. Напрями удосконалення цифровізації публічних послуг у період дії воєнного стану

Стратегічний напрям	Зміст управлінських рішень	Очікуваний системний ефект
Інституційна стандартизація цифрової екосистеми	уніфікація регуляторних вимог; запровадження єдиних стандартів інтероперабельності; чітке закріплення відповідальності за цифрові сервіси	підвищення керованості цифрової системи та зменшення фрагментації
Впровадження моделі управління цифровими ризиками	класифікація послуг за рівнем критичності; розроблення планів безперервності; регулярні стрес-тести цифрових систем	зростання адаптивності та скорочення часу відновлення сервісів
Посилення кіберстійкості державних інформаційних ресурсів	сегментація доступів; резервування дата-центрів; централізований моніторинг кіберінцидентів; аудит вразливостей	зменшення ймовірності зупинки сервісів і втрати даних
Розвиток гібридної моделі надання послуг	поєднання онлайн- та офлайн-каналів; підтримка ЦНАП як фізичного контуру безперервності; альтернативні канали ідентифікації	забезпечення доступності послуг у разі технічних або інфраструктурних збоїв
Формування цифрових і кіберкомпетентностей персоналу	системна підготовка державних службовців; сертифікація цифрових навичок; навчання з кібергігієни та захисту даних	підвищення якості адміністрування цифрових процесів
Зменшення цифрової нерівності громадян	розширення програм цифрової грамотності; підтримка вразливих груп; забезпечення доступу до цифрових інструментів у громадах	підвищення інклюзивності та довіри до цифрових сервісів
Інтеграція цифровізації у систему національної безпеки	включення цифрових платформ до стратегій стійкості; міжвідомча координація; визначення критичних сервісів як об'єктів захисту	закріплення цифрових послуг як елементу державної стійкості

Джерело: розробка авторів.

Таким чином, аналіз та систематизація викликів і загроз цифровізації публічних послуг у воєнний період дозволяє констатувати, що їхня природа має комплексний інституційно-технологічний та соціальний характер. В умовах дії воєнного стану цифрові сервіси стають елементом національної стійкості, а отже потребують переорієнтації управлінської логіки з кількісного розширення послуг на забезпечення їхньої безперервності, кіберзахищеності та інтегрованості. Це зумовлює необхідність впровадження системних управлінських рішень, спрямованих на інституційне впорядкування, технологічну стабільність та розвиток компетентнісного потенціалу персоналу публічної служби (табл. 2).

Таблиця показує, що напрями удосконалення цифровізації публічних послуг у період дії воєнного стану повинні базуватися на інтеграції інституційної впорядкованості, технологічної стійкості та компетентнісної спроможності персоналу органів публічної влади. У сучасних умовах цифрові платформи виконують функцію інфраструктури національної стійкості, а тому стратегія їх розвитку має бути орієнтована не лише на розширення переліку сервісів, але й на гарантування їхньої безперервності, безпеки та доступності. Таким чином, цифровізація публічних послуг трансформується у складову системи кризового управління та забезпечення національної безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Дослідження засвідчує, що в умовах дії воєнного стану цифровізація публічних послуг трансформується з інструменту модернізації публічного управління у складову забезпечення національної стійкості та національної безпеки. Її ефективність визначається спроможністю забезпечувати безперервність критичних сервісів, кіберзахист даних та інтегрованість міжвідомчої взаємодії. Виявлено системні інституційні, технологічні та соціально-компетентнісні ризики, що впливають на доступність і якість публічних послуг у період дії воєнного стану.

Подальші наукові розвідки доцільно зосередити на розробленні індикаторів цифрової стійкості, удосконаленні механізмів управління цифровими ризиками та дослідженні впливу цифрової нерівності на ефективність публічного управління в кризових умовах.

Література:

1. Бачинський О.-С. Я. Цифрові платформи як інструмент адаптації державних службовців в Україні. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Публічне управління та адміністрування. 2025. № 1. DOI: https://doi.org/10.32782/TNU-2663-6468/2025.1/04 https://

www.pubadm.vernadskyjournals.in.ua/journals/2025/1_2025/6.pdf

2. Завгородня Ю. В. Політика цифровізації органів місцевого самоврядування в період воєнного стану. Держава і право. 2025. Вип. 98. С. 313—323. URL: https://derzhava-i-pravo.com.ua/articles/98-313.pdf

3. Кучменко В. О., Ватульєв М. В. Цифрова трансформація публічного управління в умовах воєнного стану. Молодий вчений. 2025. № 4 (135). DOI: https://doi.org/10.32839/2304-5809/2025-4-135-14 URL: https://molodyivchenyi.ua/index.php/journal/article/view/6451/6305

4. Лопушинський І. П., Клюцевський В. І., Момоток О. М. Особливості надання публічних (електронних публічних) послуг в умовах воєнного стану в Україні. Наукові інновації та передові технології. 2023. № 4 (18). С. 110-123. https://perspectives.pp.ua/index.php/nauka/article/view/4272/4295

5. Малахова Т. Кібербезпека органів публічного управління в контексті сучасних гібридних загроз: інституційні та технологічні аспекти. Координати публічного управління. 2025. № 1 (4). С. 379—397. DOI: https://doi.org/10.62664/cpa.2025.01.18 URL: https://kpu-journal.com.ua/index.php/journal/article/view/83

6. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/67-2018-р

7. Скляр І. Особливості розвитку цифрового врядування в умовах воєнного стану. Аспекти публічного управління. 2024. Т. 12. № 4. С. 59—66. https://aspects.org.ua/index.php/journal/article/view/1093/1069

8. Шпак Ю. В., Кожина А. В., Драган І. О. Цифровізація та стандартизація у сфері публічного управління. Актуальні питання у сучасній науці. 2025. — № 3 (33). С. 440—453. DOI: https://doi.org/10.52058/2786-6300-2025-3(33)-440-453 URL: https://perspectives.pp.ua/index.php/sn/article/view/21392/21366

9. Gustafsson M., Matveieva O., Wihlborg E., Borodin Y., Mamatova T., Kvitka S. Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine. Government Information Quarterly. 2025. Vol. 42, Issue 3. DOI: https://doi.org/10.1016/j.giq.2025.102056 URL: https://www.sciencedirect.com/science/article/pii/S0740624X25000504

10. Public administration in Ukraine: assessment against the Principles of Public Administration. Paris: OECD Publishing, 2023. 212 p. OECD URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/public-administration-in-ukraine_27a46a58/078d08d4-en.pdf

11. Trembita.gov.ua — report for the 1st quarter of 2023 / EU4DigitalUA project. 2023. URL: https://eu4digitalua.eu/en/news/trembita-gov-ua-report-for-the-1st-quarter-of-2023/

12. Trembita.gov.ua — report for the 3d quarter of 2025 / EU4DigitalUA project. 2025. URL: https://eu4digitalua.eu/uk/news/trembita-gov-ua-zvit-za-3-j-kvartal-2025-roku/

References:

1. Bachynskyi, O.-S.Ya. (2025), "Digital platforms as a tool for adaptation of civil servants in Ukraine", Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia, vol. 1. https://doi.org/10.32782/TNU-2663-6468/2025.1/04

2. Zavhorodnia, Yu.V. (2025), "Policy of digitalization of local self-government bodies during martial law", Derzhava i pravo, vol. 98, p. 313—323.

3. Kuchmenko, V.O. and Vatuliev, M.V. (2025), "Digital transformation of public administration under martial law", Molodyi vchenyi, vol. 135, no. 4. https://doi.org/10.-32839/2304-5809/2025-4-135-14

4. Lopushynskyi, I.P., Kliutsevskyi, V.I. and Momotok, O.M. (2023), "Features of providing public (electronic public) services under martial law in Ukraine", Naukovi innovatsii ta peredovi tekhnolohii, vol. 18, no. 4, p. 110—123.

5. Malakhova, T. (2025), "Cybersecurity of public administration bodies in the context of modern hybrid threats: institutional and technological aspects", Koordynaty publichnoho upravlinnia, vol. 4, no. 1. https://doi.org/10.62664/cpa.2025.01.18

6. Cabinet of Ministers of Ukraine (2018), "On approval of the Concept for the development of the digital economy and society of Ukraine for 2018—2020 and approval of the action plan for its implementation", available at: https://zakon.rada.gov.ua/go/67-2018-%D1%80 (Accessed 25 Feb 2026).

7. Skliar, I. (2024), "Features of the development of digital governance under martial law", Aspekty publichnoho upravlinnia, vol. 12, no. 4, p. 59—66.

8. Shpak, Yu.V., Kozhyna, A.V. and Dragan, I.O. (2025), "Digitalization and standardization in the field of public administration", Aktualni pytannia u suchasnii nautsi, vol. 33, no. 3. https://doi.org/10.52058/2786-6300-2025-3(33)-440-453

9. Gustafsson, M., Matveieva, O., Wihlborg, E., Borodin, Y., Mamatova, T. and Kvitka, S. (2025), "Adaptive governance amidst the war: overcoming challenges and strengthening collaborative digital service provision in Ukraine", Government Information Quarterly, vol. 42, no. 3. https://doi.org/10.1016/j.giq.2025.102056

10. OECD (2024), Public administration in Ukraine: assessment against the Principles of Public Administration, OECD Publishing, Paris, available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/public-administration-in-ukraine_27a46a58/078d08d4-en.pdf (Accessed 25 Feb 2026).

11. EU4DigitalUA (2023), "Trembita.gov.ua — report for the 1st quarter of 2023", available at: https://eu4digitalua.eu/en/news/trembita-gov-ua-report-for-the-1st-quarter-of-2023/ (Accessed 25 Feb 2026).

12. EU4DigitalUA (2026), "Trembita.gov.ua — report for the 1st quarter of 2025", available at: https://eu4digitalua.eu/uk/news/trembita-gov-ua-zvit-za-3-j-kvartal-2025-roku/ (Accessed 25 Feb 2026).

Отримано редакцією журналу / Received: 07. 03.26
Прорецензовано / Revised: 13. 03.26
Схвалено до друку / Accepted:17.03.26