РОЗДІЛ 1
ТЕОРІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 351:004.9:323.2(477)
DOI https://doi.org/10.51547/ppp.dp.ua/2024.4.1

Кравцов Олег Валентинович,
кандидат хімічних наук,
доцент кафедри державного управління і місцевого самоврядування
Національного технічного університету «Дніпровська політехніка»
ORCID ID: 0000-0002-8027-1796

РОЛЬ ДЕРЖАВНОГО УПРАВЛІННЯ В РОЗБУДОВІ НАЦІОНАЛЬНОЇ МОДЕЛІ СТІЙКОСТІ В ЦИФРОВОМУ СУСПІЛЬСТВІ

THE ROLE OF PUBLIC ADMINISTRATION IN BUILDING A NATIONAL MODEL OF RESILIENCE IN THE DIGITAL SOCIETY

У статті досліджено сучасні виклики, які постають перед державами у цифрову еру, визначено роль державного управління у забезпеченні національної стійкості в умовах стрімких цифрових трансформацій. Доведено, що цифровізація спричиняє як нові можливості для розвитку, так і потенційні загрози, що зумовлюють необхідність створення гнучких і ефективних механізмів захисту національних інтересів.

Проаналізовано ключові аспекти впливу державного управління на формування та підтримку стійкості системи, а також виявлено, що інтеграція між різними секторами (державними органами, науковими установами, бізнес-середовищем і громадськістю) є важливим чинником у мінімізації цифрових ризиків. Встановлено, що такі партнерські взаємодії сприяють розробці інноваційних рішень, які забезпечують швидку адаптацію до змін і підвищують ефективність реагування на цифрові виклики.

У статті обґрунтовано необхідність впровадження міждисциплінарного підходу як основи для якісного прогнозування майбутніх загроз і розробки управлінських рішень, що забезпечують стійкість. Запропоновано модель поєднання моніторингу ризиків та впровадження прозорих механізмів контролю цифрової безпеки, що сприяє ранньому виявленню загроз і економії ресурсів на етапах їх ліквідації. Результати дослідження підтверджують, що ефективне державне управління має вирішальне значення для інтеграції аспектів цифрової стійкості. Здійснено детальний аналіз механізмів взаємодії між зацікавленими сторонами, які формують загальнонаціональну стратегічну відповідь на ризики, пов'язані з глобальною цифровою трансформацією.

У статті акцентовано увагу на важливості створення систем моніторингу та контролю за дотриманням стандартів цифрової безпеки. Встановлено, що такі системи покращують координацію між державними органами та забезпечують гнучкість у реагуванні на сучасні виклики цифрового середовища. Узагальнено, що державне управління в умовах цифровізації є непересічним інструментом для збереження сталості системи, мінімізації ризиків і впровадження стратегій адаптації до нових технологій у рамках національної безпеки та розвитку.

Ключові слова: *цифрова стійкість, цифрове суспільство, міждисциплінарний підхід, управлінські механізми.*

The article examines the current challenges faced by states in the digital era and defines the role of public administration in ensuring national sustainability in the context of rapid digital transformations. It is proved that digitalisation creates both new opportunities for development and potential threats, which necessitate the creation of flexible and effective mechanisms for protecting national interests.

The author analyses the key aspects of the impact of public administration on the formation and maintenance of system resilience, and reveals that integration between different sectors (government agencies, academic institutions, business environment and the public) is an important factor in minimising digital risks. It is established that such partnerships contribute to the development of innovative solutions that ensure rapid adaptation to changes and increase the effectiveness of responding to digital challenges.

The article substantiates the need to introduce an interdisciplinary approach as a basis for qualitative forecasting of future threats and development of management solutions that ensure sustainability. A model of combining risk monitoring and implementation of transparent digital security control mechanisms is proposed, which facilitates early detection of threats and saves resources at the stages of their elimination. The results of the study confirm that effective public administration is crucial for integrating aspects of digital resilience. A detailed analysis of the mechanisms of interaction between stakeholders that form a national strategic response to the risks associated with global digital transformation is carried out.

The article focuses on the importance of creating systems for monitoring and controlling compliance with digital security standards. It is established that such systems improve coordination between government agencies and provide flexibility in responding to the current challenges of the digital environment. It is generalised that public administration in the context of digitalisation is an outstanding tool for maintaining system sustainability, minimising risks and implementing strategies for adapting to new technologies within the framework of national security and development.

Key words**:** *digital sustainability, digital society, interdisciplinary approach, governance mechanisms.*

Постановка проблеми. Цифровізація є основним драйвером розвитку сучасного суспільства, впливаючи на економіку, соціальні відносини та державне управління. Інтеграція цифрових технологій трансформує взаємодію громадян із державними інституціями, бізнесом і між собою. У цих умовах головним завданням стає створення стійкої моделі управління цифровими процесами, що забезпечить зменшення ризиків і використання нових можливостей цифровізації.

Цифрові технології відкривають широкі перспективи, серед яких автоматизація, підвищення ефективності управлінських рішень, доступ до інноваційних сервісів і послуг. Водночас стрімка цифровізація породжує низку загроз, що потребують негайної уваги. Зокрема, збільшення кількості кіберзагроз піддає ризику безпеку критичної інфраструктури. Нерівний доступ до технологій створює ймовірність соціальної маргіналізації, обмежуючи участь у цифровій економіці значної частини населення. Накопичення великих обсягів даних вимагає розробки механізмів їхнього ефективного регулювання. Виклики, пов'язані із захистом персональної інформації, прозорістю використання даних та запобіганням їхнім зловживанням, залишаються актуальними для державної політики.

Аналіз останніх досліджень і публікацій. Аналіз наукових праць демонструє багатогранний підхід до вивчення формування національної стійкості, охоплюючи різні аспекти: інформаційно-психологічні чинники, механізми державного управління, цифрові ініціативи та правові основи електронного врядування. На думку В. Бондаря [1], національна стійкість є невіддільною частиною системи національної безпеки, зокрема, через вплив інформаційно-психологічного чинника, що підвищує здатність адаптуватися до динамічного середовища загроз. О. О. Резнікова [2] зосереджується на необхідності вдосконалення методів управління для забезпечення стійкості в мінливому безпековому середовищі.

Як зазначає В. Александров [3], підтримка національної стійкості потребує стратегічного й тактичного планування в межах публічного управління. Комплексний підхід, розроблений З. Ковалем і С. Пововим [4], передбачає поєднання стратегій активної оборони та стійких асиметричних дій в умовах інформаційно-психологічної епохи. Дослідження М. В. Міляєвої [13] підкреслює важливість адаптації нормативного середовища для впровадження електронного врядування, яке має вирішальне значення для ефективності державного управління. А. Богоніс [15] акцентує на викликах цифровізації, які потребують інноваційних підходів до їхнього подолання.

Міжнародний досвід, представлений у дослідженнях S. Abbasi та B. K. Jung [16], висвітлює важливі ініціативи цифрового здоров'я, спрямовані на формування стійкості до пандемій. Виклики цифрової трансформації та шляхи їхнього вирішення обговорюються в роботах F. Brunetti та співавторів [17], які пропонують багатосторонні стратегії для адаптації до сучасних умов.

Виділення невирішених раніше частин загальної проблеми. Попри значні досягнення в дослідженні ролі державного управління у формуванні національної стійкості, деякі аспекти залишаються недостатньо висвітленими. Зокрема, не звертається належної уваги на інтеграцію різних аспектів цифрової стійкості, а також застосування міждисциплінарного підходу для комплексного аналізу викликів і ризиків. Додатково необхідно акцентувати на довгострокових ефектах цифровізації та прогнозуванні майбутніх загроз, які можуть суттєво впливати на стійкість суспільства. Ця робота спрямована на подолання невирішених раніше частин загальної проблеми, зокрема, недостатньої уваги до інтеграції різних аспектів цифрової стійкості та відсутності міждисциплінарного підходу для комплексного аналізу викликів і ризиків.

Мета статті – аналіз ролі державного управління у формуванні стійкості цифрового суспільства, що передбачає аналіз нормативно-правової бази та інституційних механізмів, що сприяють забезпеченню цифрової стійкості, дослідження міжнародного досвіду у розбудові стійкості цифрового суспільства та оцінки його потенційну адаптацію для України.

Виклад основного матеріалу. Концепт «національна стійкість» виник як наслідок змін підходів до захисту національної безпеки та розвитку теорії систем. Його інтеграція в систему національної безпеки зумовлена необхідністю прийняття оперативних управлінських рішень для своєчасного та ефективного реагування на широкий спектр загроз і кризових ситуацій, включаючи протидію деструктивним процесам у державі та суспільстві в умовах інтенсивної гібридної фази та її інформаційних аспектів [1, 480]. Національну стійкість можна трактувати як здатність держави, суспільства та окремих громадян адаптуватися до змін, викликаних цифровізацією, протистояти зовнішнім і внутрішнім загрозам, а також забезпечувати сталий розвиток у цифровому середовищі [2].

Основними елементами національної стійкості можна визначити адаптивність, тобто здатність держави та суспільства швидко пристосовуватись до змін та викликів; опірність – спроможність чинити ефективний опір внутрішнім і зовнішнім загрозам; стабільність – здатність зберігати функціонування та мінімізувати негативні наслідки під час кризових ситуацій; а також відновлюваність – можливість швидко відновлюватися після криз, повертаючи економічні, соціальні та інституційні показники на попередній рівень або навіть вищий [3, 27]. Ці елементи сприяють забезпеченню сталого розвитку та стійкості держави в умовах динамічних змін і викликів сучасного світу.

Державне управління є основним інструментом у формуванні національної стійкості, здатним як посилювати, так і послаблювати ефективність інших підсистем у протистоянні негативним впливам глобальних ризиків. Воно відповідає за розробку та впровадження відповідної моделі забезпечення національної стійкості. Важливо зазначити, що будь-яка така модель повинна бути динамічною, постійно адаптуючись до змін у зовнішньому та внутрішньому середовищі. Процес забезпечення національної стійкості потребує регулярного уточнення та оновлення, включаючи впровадження нових механізмів, таких як інформаційно-психологічні методи, які набувають особливої актуальності в сучасних умовах [4, 102].

Цифрове суспільство створює унікальні можливості для розвитку, проте одночасно формує нові виклики, які вимагають ретельного аналізу та стратегічного підходу. Здатність держави ефективно реагувати на ці виклики є визначальним фактором забезпечення національної стійкості в умовах цифрової трансформації(табл. 1).

Одним із фундаментальних елементів забезпечення цифрової стійкості є створення та розвиток нормативно-правової бази, яка визначає правові рамки функціонування інформаційних технологій. В Україні основними в цій сфері є закони та підзаконні акти, що регулюють кібербезпеку, електронне урядування, захист персональних даних, електронну комерцію та цифрову інфраструктуру. Ефективна нормативно-правова база повинна враховувати як внутрішні потреби держави, так і міжнародні стандарти, зокрема рекомендації Європейського Союзу, Організації Об'єднаних Націй та Міжнародного союзу електрозв'язку.

Регулювання цифрових процесів є ще одним важливим аспектом діяльності держави. Аналіз законодавства показує, що Україна зробила суттєві кроки в напрямку цифровізації, включаючи ухвалення низки нормативних актів, які створюють необхідні правові засади для розвитку цифрових платформ, гарантування кібербезпеки та захисту даних. Закон України «Про основні засади забезпечення кібербезпеки України» [5] – основний, що визначає головні положення у сфері підтримки кібербезпеки, установлює права та обов'язки суб'єктів у сфері захисту інформації, а також встановлює правила взаємодії держав-

Таблиця 1

Виклики цифрового суспільства

Виклики цифрового суспільства	Опис викликів
Кіберзагрози та безпека даних	Зростання кількості кіберзлочинів, ризик втрати або викрадення критично важливої інформації
Проблеми цифрової нерівності	Нерівний доступ до цифрових технологій, який посилює соціальну нерівність та обмежує цифрову інклюзію
Управління критичною цифровою інфраструктурою	Необхідність захисту цифрової інфраструктури, включно з енергетикою, телекомунікаціями та транспортом
Регулювання цифрових технологій і захист персональних даних	Виклики, пов'язані з прозорістю, безпекою та конфіденційністю у використанні цифрових рішень

Джерело: створено авторами

них органів та приватного сектору для підвищення стійкості до кіберзагроз. Закон України «Про електронні довірчі послуги» [6] забезпечує правові основи для використання електронних довірчих послуг, таких як електронні підписи, печатки та інші методи автентифікації в цифровому середовищі. Це сприяє створенню безпечного середовища для обміну інформацією та підвищенню довіри до електронних процесів. Закон України «Про захист персональних даних» [7] визначає основні принципи обробки персональних даних та створює умови для їхнього захисту; сприяє гарантуванню конфіденційності, безпеки та контролю за обробкою персональної інформації, що є важливим для дотримання прав людини в цифровому суспільстві. Закон України «Про електронні комунікації» [8] регулює питання функціонування електронних комунікаційних мереж та послуг, сприяючи створенню конкурентного середовища на ринку цифрових послуг, що забезпечує їхню доступність та якість для всіх категорій користувачів.

Гармонізація із міжнародними стандартами є визначальним елементом державного управління у формуванні цифрової стійкості. У контексті європейської інтеграції Україна активно адаптує національне законодавство до норм Європейського Союзу (ЄС). Зокрема, упровадження положень Загального регламенту захисту даних (GDPR) [9] стало значним кроком у підвищенні рівня захисту персональних даних і забезпеченні прозорості цифрових процесів. Крім того, Україна бере участь в ініціативах Організації Об'єднаних Націй (ООН), спрямованих на розвиток інформаційного суспільства, таких як Цілі сталого розвитку [10], що охоплюють цифрову інклюзію та доступ до інформаційних технологій.

Національна гармонізація із міжнародними стандартами також передбачає дотримання рекомендацій Міжнародного союзу електрозв'язку (ITU) [11] щодо розвитку цифрової інфраструктури, зокрема широкосмугового інтернету, та участь у глобальних ініціативах із кібербезпеки. Це сприяє інтеграції України у світову цифрову екосистему, забезпечуючи доступ до передових технологій і знань.

Інституційні механізми забезпечення цифрової стійкості в Україні базуються на координації діяльності органів державної влади, приватного сектору, наукових установ та громадянського суспільства. Серед основних органів державного управління, відповідальних за цифрову трансформацію в Україні, особливе місце посідає Міністерство цифрової трансформації України, що займається реалізацією державної політики у сфері цифровізації, включаючи впровадження електронного урядування, розвиток цифрової інфраструктури, гарантування кібербезпеки та популяризацію цифрової грамотності серед населення. Крім того, важливу роль відіграють такі інституції, як Державна служба спеціального зв'язку та захисту інформації, яка відповідає за захист кібербезпеки, а також Національний координаційний центр кібербезпеки, що здійснює оперативну координацію у випадках загроз.

Співпраця між органами влади на національному рівні доповнюється партнерством із міжнародними організаціями, такими як Європейська комісія, НАТО та ООН, що дає можливість інтегрувати кращі світові практики у сферу цифрової трансформації. Зокрема, участь у міжнародних проєктах, таких як European Interoperability Framework (EIF) [12], допомагає гармонізувати цифрові послуги з європейськими стандартами.

Держава активно інвестує в розвиток цифрової інфраструктури, яка є базовою умовою для забезпечення доступу до сучасних технологій у всіх регіонах країни. Завдяки доступу до різноманітних державних електронних послуг громадяни матимуть змогу активно брати участь у суспільному житті та демократичних процесах, а бізнес – ефективно розвиватися та адаптуватися до сучасних умов [13, 42]. Важливими напрямами є розширення мережі широкосмугового інтернету, упровадження 5G-технологій та модернізація центрів обробки даних. Інвестиції в ці сфери сприяють подоланню цифрової нерівності, що є основним викликом для багатьох країн, включно з Україною. У рамках проєкту EU4DigitalUA спільно з ЄС та естонською Академією електронного управління, Україна продовжує розбудову інфраструктури цифрового уряду, електронних державних послуг, кібербезпеки та захисту даних, використовуючи цифрові інструменти для подолання викликів, пов'язаних із війною. На початок квітня 2024 року було завершено впровадження трьох компонентів проєкту ЄС із бюджетом 10 млн євро, які стосуються розвитку інтероперабельності та інфраструктури цифрового уряду, створення електронних послуг та підтримки кібербезпеки [14].

За підтримки EU4DigitalUA впродовж чотирьох років було масштабовано систему «Трембіта», що дало змогу здійснити 5 млрд безпечних обмінів даними між державними інформаційними системами завдяки модернізації десяти основних державних реєстрів. Також було

створено платформу Diia.Engine, упроваджено 59 вебсервісів та 66 вебклієнтів на основі цієї системи. Крім того, проєкт EU4DigitalUA долучився до розвитку 54 електронних послуг, серед яких: «е-Підприємець», «uResidency», цифрові COVID-сертифікати, витяги про несудимість, можливість подання заяви про укладання шлюбу в «Дії» тощо [14]. Інтеграція штучного інтелекту в цифрові системи вимагає значної адаптації ІТ-інфраструктури й оновлення нормативної бази. Уряди змушені модернізувати закони щодо захисту даних, кібербезпеки та етичних стандартів для ефективного використання цих технологій. Ця адаптація включає створення програм навчання, спрямованих на підготовку кадрів із необхідними навичками для роботи в сучасному високотехнологічному цифровому середовищі [15, 274]. Таким чином, взаємодія з приватним сектором, громадськими організаціями, технологічна підтримка, інвестиції в цифрову інфраструктуру та стимулювання інновацій є взаємопов'язаними елементами цифрової стійкості. Комплексний підхід до цих аспектів забезпечує сталість розвитку в умовах швидкої цифровізації.

Вивчення прикладів таких країн, як Естонія, Сингапур та Ізраїль, дає змогу зрозуміти визначальні чинники, що сприяють досягненню цифрової стійкості, а їхній досвід – визначити конкретні практики, які можуть бути адаптовані до українських реалій (табл. 2).

Україна має всі передумови для успішного впровадження найкращих практик формування цифрової стійкості. Досвід Естонії в електронному урядуванні, ініціативи Сингапуру в упровадженні розумних технологій та інноваційні підходи Ізраїлю до кібербезпеки й стартап-екосистеми можуть стати основою для формування національної моделі цифрової трансформації. Для цього важливо зосередитися на гармонізації з міжнародними стандартами, інвестиціях у цифрову інфраструктуру, посиленні державно-приватного партнерства й розвитку цифрових компетенцій населення.

Державно-приватне партнерство є основним для розвитку цифрової економіки, що дає змогу об'єднати ресурси та знання для реалізації великих цифрових проєктів, що сприяє модернізації інфраструктури та розвитку інновацій. Створення спеціальних програм співпраці для бізнесу й держави дасть можливість забезпечити гнучкість й адаптивність до змін. Отже, удосконалення державного управління через цифровізацію, розвиток компетенцій, моніторинг загроз і партнерство з приватним сектором є основними напрямами формування цифрової стійкості в Україні.

Висновки. Таким чином, національна стійкість у цифровому суспільстві є складною багатокомпонентною системою, яка потребує скоординованих зусиль держави, бізнесу та громадян. Її забезпечення вимагає інноваційного підходу до управління, глибокого розуміння цифрових викликів і готовності до швидкої адаптації в динамічному середовищі.

Практичні рекомендації для України зосереджуються на вдосконаленні державного управління в умовах цифровізації, забезпеченні стійкості цифрового суспільства та впровадженні новітніх технологій. Важливим аспектом є створення ефективних механізмів державно-приватного партнерства, розвиток цифрових навичок серед державних службовців, а також упровадження сучасних систем моніторингу цифрових загроз.

Перспективи подальших досліджень включають глибший аналіз регуляторних практик,

Таблиця 2

Міжнародний досвід: приклади країн, які успішно впроваджують цифрову стійкість

Країна	Основні досягнення	Уроки для України
Естонія	Повна цифровізація державних послуг, упровадження системи e-Residency, високий рівень кібербезпеки	Адаптація досвіду електронного урядування, зокрема, створення єдиної платформи для цифрових послуг та вдосконалення системи кіберзахисту
Сингапур	Розвиток Smart Nation Initiative: інтеграція IoT в міське управління, інвестиції в цифрову грамотність	Використання IoT для управління інфраструктурою, розширення цифрових навичок серед громадян, упровадження «розумних» рішень у міському середовищі
Ізраїль	Лідерство у сфері кібербезпеки, інноваційний підхід до стартап-екосистеми, стратегічне державно-приватне партнерство	Розвиток стартап-інкубаторів, стимулювання державно-приватного партнерства у сфері кібербезпеки, інвестування в освіту для підготовки фахівців

Джерело: створено авторами на основі [16].

адаптацію міжнародного досвіду до українських умов, а також вивчення інноваційних підходів у сфері цифрової трансформації. Це сприятиме забезпеченню сталості й розвитку цифрового середовища, яке відповідає сучасним викликам та є інтегрованим у глобальні цифрові процеси.

REFERENCES:

1. Bondar, V. (2024). Natsionalna stiikist v systemi natsionalnoi bezpeky: informatsiino-psykholohichnyi chynnyk [National resilience in the national security system: informational and psychological factor]. *Suspilstvo ta natsionalni interesy – Society and National Interests, 5*(5). https://doi.org/10.52058/3041-1572-2024-5(5)-477-487 [in Ukrainian].
2. Reznikova, O. O. (2022). Natsionalna stiikist v umovakh minlyvoho bezpekovoho seredovyshcha [National resilience in a changing security environment]. Kyiv: NISD. Retrieved from https://www.marshallcenter.org/sites/default/files/files/2022-04/Reznikova_Resilience_UKR.pdf [in Ukrainian].
3. Aleksandrov, V. (2022). Osnovni naukovi pidkhody shchodo publichnoho upravlinnia zabezpechennia natsionalnoi stiikosti Ukrainy [Basic scientific approaches to public management of ensuring Ukraine's national resilience]. *Naukovi perspektyvy (Naukovì perspektivi), 9*(27). https://doi.org/10.52058/2708-7530-2022-9(27)-21-34 [in Ukrainian].
4. Koval, Z., & Povov, S. (2021). Kompleksnyi mekhanizm derzhavnoho upravlinnia: natsionalna doktryna stiikosti Ukrainy, stratehiia stiikoi ta aktyvnoi oborony, taktyka stiikykh asymetrychnykh dii v informatsiino-psykholohichnu epokhu [Comprehensive state governance mechanism: national doctrine of Ukraine's resilience, strategy of sustainable and active defense, tactics of resilient asymmetric actions in the informational and psychological era]. *Aktualni problemy derzhavnoho upravlinnia – Current Problems of Public Administration, 3*(84), 99–104. https://doi.org/10.35432/1993-8330appa3842021246296 [in Ukrainian].
5. Verkhovna Rada of Ukraine. (October 5, 2017). On the Basic Principles of Cybersecurity in Ukraine: Law of Ukraine No. 2163-VIII (as of June 28, 2024). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Verkhovna Rada of Ukraine. (October 5, 2017). On Electronic Trust Services: Law of Ukraine No. 2155-VIII (as of December 18, 2024). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#Text
7. Verkhovna Rada of Ukraine. (June 1, 2010). On Personal Data Protection: Law of Ukraine No. 2297-VI (as of April 27, 2024). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Verkhovna Rada of Ukraine. (December 16, 2020). On Electronic Communications: Law of Ukraine No. 1089-IX (as of November 15, 2024). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20#Text
9. General Data Protection Regulation (GDPR). Retrieved from https://gdpr-info.eu/
10. United Nations Development Programme (UNDP). (2024). Shcho take Tsili staloho rozvytku? [What are the Sustainable Development Goals?]. Retrieved from https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku [in Ukrainian].
11. Ministry of Foreign Affairs of Ukraine. (2024). Mizhnarodnyi soiuz elektroviazku (MSE) [International Telecommunication Union (ITU)]. Retrieved from https://geneva.mfa.gov.ua/posolstvo/2616-itu [in Ukrainian].
12. European Commission. (2024). *The European Interoperability Framework*. Retrieved from https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail
13. Miliayeva, M. V. (2024). Administratyvno-pravove zabezpechennia rozbudovy elektronnoho vriaduvannia [Administrative and legal support for the development of e-governance]. *Expert Paradigm of Law and Public Administration, 2*(30), 39–45. https://doi.org/10.32689/2617-9660-2024-2(30)-39-45 [in Ukrainian].
14. National Institute for Strategic Studies (NISS). (2024). Tsyfrova transformatsiia ekonomiky Ukrainy v umovakh viiny [Digital transformation of Ukraine's economy during the war]. Retrieved from https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-kviten-2024 [in Ukrainian].
15. Bohonis, A. (2024). Tsyfrovizatsiia informatsii: novi vyklyky v systemi derzhavnoho upravlinnia [Digitalization of information: New challenges in the system of public administration]. *Uspikhy i dosiahennia u nautsi – Successes and Achievements in Science, 5*(5). https://doi.org/10.52058/3041-1254-2024-5(5)-269-276 [in Ukrainian].
16. Abbasi, S., & Jung, B. K. (2023). Mapping of key digital health initiatives building resilience for current and future pandemics. *Mapping of Key Digital Health Initiatives Building Resilience for Current and Future Pandemics*, 1–23. Retrieved from https://ieeexplore.ieee.org/abstract/document/10026166/authors#authors
17. Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal*, *32*(4), 697–724. https://doi.org/10.1108/tqm-12-2019-0309