УДК 35.351
DOI https://doi.org/10.51547/ppp.dp.ua/2025.3.5

Міщенко Дмитро Анатолійович,
доктор наук з державного управління, професор,
професор кафедри маркетингу
Університету митної справи та фінансів
ORCID ID: 0000-0003-0278-7209

Міщенко Людмила Олександрівна,
кандидат економічних наук, доцент,
доцент кафедри економіки та менеджменту
ЗВО ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-0163-0763

Хурдей Вікторія Дмитрівна,
кандидат економічних наук, доцент,
завідувач кафедри маркетингу
Університету митної справи та фінансів
ORCID ID: 0000-0001-9210-9705

ЦИФРОВІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ ЯК ЧИННИК НЕЙТРАЛІЗАЦІЇ ЗАГРОЗ НАЦІОНАЛЬНИМ ІНТЕРЕСАМ

DIGITALIZATION OF PUBLIC ADMINISTRATION AS A FACTOR IN NEUTRALIZING THREATS TO NATIONAL INTERESTS

Стаття присвячена аналізу ролі цифровізації публічного управління у зміцненні національної безпеки України, особливо у контексті протистояння гібридним загрозам. Автори обґрунтовують тезу, що цифрові інструменти є ключовим фактором стійкості держави в умовах сучасних викликів, зокрема інформаційної війни, дезінформації, кібератак та спроб дестабілізації політичної системи.

На основі аналізу міжнародного досвіду окреслено ефективні цифрові практики, що поєднують елементи прозорого управління, кібербезпеки, електронної демократії та стратегічної комунікації. Увагу приділено українському контексту – розвитку екосистеми «Дія», інтеграції цифрових сервісів, проблемам цифрової довіри та кіберопору. Стаття пропонує напрямки адаптації успішних міжнародних моделей до українських реалій з урахуванням політичних, технологічних та безпекових викликів. У підсумку автори підкреслюють важливість формування цифрової стійкості як нової парадигми публічного управління у XXI столітті. На основі вивчення міжнародних кейсів (Естонія, Ізраїль, Литва, Фінляндія) виокремлено найефективніші практики, що охоплюють такі напрями як побудова прозорих систем електронного урядування (наприклад, архітектура X-Road для захисту критично важливих даних, розвиток систем проактивного кіберзахисту та підвищення медіаграмотності населення.

Детально аналізуються виклики, з якими стикається Україна на шляху цифрової трансформації: дефіцит кваліфікованих кадрів, необхідність удосконалення законодавчої бази, постійні кіберзагрози та інформаційні атаки, а також потреба інтеграції безпекового підходу «security by design» на всіх рівнях. Підкреслюється, що цифровізація має розглядатися не лише як засіб підвищення ефективності державного управління, а й як стратегічний компонент національної безпеки, здатний забезпечити функціонування держави в кризових умовах. Розглядається використання електронних послуг для підтримки внутрішньо переміщених осіб, реалізація програм компенсацій за зруйноване житло, а також сервіси документаційного супроводу. Стаття пропонує комплексну модель цифрової стійкості, що поєднує технічні, організаційні та соціальні аспекти. Автори обґрунтовують необхідність системного моніторингу ефективності цифрових рішень, проведення глибинних досліджень впливу цифрових сервісів на довіру громадян до влади та розробки методологій оцінки цифрової зрілості інституцій.

Ключові слова*: *цифрове публічне управління, загрози, електронна демократія, кібербезпека, національна стійкість, національні інтереси, стратегічні комунікації, цифрова трансформація, інформаційна безпека.

The article examines the role of the digitalization of public administration in strengthening Ukraine's national security, particularly in the context of countering hybrid threats. The authors substantiate the thesis that digital tools are a key factor in

state resilience amid contemporary challenges, including information warfare, disinformation, cyberattacks, and attempts to destabilize the political system.

Based on an analysis of international experience, the article outlines effective digital practices that combine elements of transparent governance, cybersecurity, e-democracy, and strategic communication. Special attention is given to the Ukrainian context–the development of the Diia ecosystem, the integration of digital services, and the issues of digital trust and cyber resilience. The article proposes directions for adapting successful international models to Ukrainian realities, taking into account political, technological, and security challenges. In conclusion, the authors emphasize the importance of building digital resilience as a new paradigm of public administration in the 21st century. Drawing on international case studies (Estonia, Israel, Lithuania, Finland), the article identifies the most effective practices, including the construction of transparent e-government systems (for example, the X-Road architecture), the protection of critical data, the development of proactive cyber defense systems, and the enhancement of public media literacy.

The article provides a detailed analysis of the challenges Ukraine faces on the path of digital transformation: a shortage of qualified personnel, the need to improve the legal framework, persistent cyber threats and information attacks, and the necessity of integrating a "security by design" approach at all levels. It is emphasized that digitalization should be considered not only as a means of improving the efficiency of public administration but also as a strategic component of national security, capable of ensuring the functioning of the state under crisis conditions. The discussion covers the use of e-services to support internally displaced persons, the implementation of compensation programs for destroyed housing, and documentation support services. The article proposes a comprehensive model of digital resilience that integrates technical, organizational, and social dimensions. The authors justify the need for systematic monitoring of the effectiveness of digital solutions, conducting in-depth studies on the impact of digital services on public trust in government, and developing methodologies for assessing the digital maturity of institutions.

Key words**:** *digital public administration, threats, e-democracy, cybersecurity, national resilience, national interests, strategic communications, digital transformation, information security.*

Вступ. В умовах зростання масштабів загроз національним інтересам, що охоплюють інформаційні атаки, кіберінциденти, спроби підриву легітимності державної влади, особливої актуальності набуває переосмислення ролі цифрового публічного управління як системної відповіді на нові виклики безпеці. Водночас в Україні ще недостатньо досліджено, яким чином цифрові інструменти можуть підвищувати стійкість політичної системи та забезпечувати захист національних інтересів.

Мета статті – проаналізувати цифрове публічне управління як інструмент зміцнення національної стійкості до сучасних загроз на основі міжнародного досвіду та окреслити перспективи його ефективної імплементації.

Проблематика цифрового врядування, кібербезпеки та публічного управління в умовах загроз національним інтересам поступово набирає ваги в науковому дискурсі. У дослідженнях українських і зарубіжних авторів (Ю. Ганущак, В. Липкан, T. Janowski, M. Castells, M. Dunleavy) аналізуються питання впровадження цифрових сервісів, забезпечення кіберзахисту, підвищення відкритості управління. Водночас більшість праць зосереджена на технічному або організаційному аспектах цифровізації, уникаючи комплексного аналізу її потенціалу в забезпеченні захисту національних інтересів. Наявний розрив між цифровими інноваціями та безпековими стратегіями актуалізує необхідність нових підходів до розуміння цифрового публічного управління як інструменту захисту політичної стабільності, довіри до влади та державної цілісності.

Результати дослідження. У сучасному геополітичному ландшафті держави стикаються з дедалі складнішими та багатовимірними загрозами, які часто мають гібридний характер. Ці загрози охоплюють не лише традиційні військові конфлікти, а й інформаційні, кібернетичні, економічні та політичні впливи, спрямовані на дестабілізацію внутрішньої ситуації, підрив довіри до державних інституцій та ослаблення міжнародних позицій. У цьому контексті цифрове публічне управління постає як ключовий інструмент для зміцнення стійкості держави, здатності ефективно протистояти загрозам та забезпечувати національну безпеку [2].

Гібридні загрози, орієнтовані на політичну сферу, мають на меті підірвати легітимність влади, спровокувати внутрішню нестабільність та розколоти суспільство. До основних з них належать:

– інформаційно-психологічні операції (ІПСО), що полягають у поширенні дезінформації, фейкових новин, пропаганди з метою маніпулювання громадською думкою, дискредитації державних інститутів, посиленні поляризації суспільства та створенні хаосу. Вони можуть включати використання соціальних мереж, ботів, тролів та цілеспрямованих кібератак на інформаційні ресурси. Сучасні ІПСО стають дедалі витонченішими завдяки використанню штучного інтелекту та «deepfake» технологій, що ускладнює їх ідентифікацію;

– кібератаки на державні інституції та критичну інфраструктуру, включають цілеспрямовані атаки на урядові сайти, бази даних, системи життєзабезпечення (енергетика, транспорт, фінанси) з метою паралізації їх роботи, викрадення конфіденційних даних або руйнування інфраструктури. Такі атаки можуть мати як руйнівний, так і шпигунський характер, підриваючи функціонування держави та довіру громадян до її здатності забезпечувати безпеку;

– втручання у виборчі процеси, здійснюється у вигляді впливу на результати виборів шляхом маніпулювання даними, поширення компрометуючої інформації про кандидатів, організації DDoS-атак на виборчі системи або використання мереж ботів для формування потрібних настроїв;

– економічний тиск та корупція, тобто використання економічних важелів, таких як торговельні ембарго, санкції, енергетичний шантаж, для дестабілізації економіки держави. Корупційна загроза в даному контексті полягає у заохоченні та використанні корупції в державних структурах для підриву довіри до влади та створенні внутрішніх конфліктів;

– ініціювання соціальних та політичних заворушень, стимулювання протестних настроїв, етнічних або релігійних конфліктів, використання вразливих груп населення для організації масових заворушень та дестабілізації внутрішньополітичної ситуації [5].

Роль цифрової трансформації публічного управління в підвищенні стійкості держави проявляється в тому, що цифрова трансформація є не просто модернізацією державних послуг, а комплексною переорієнтацією всіх аспектів державного управління на використання цифрових технологій для підвищення ефективності, прозорості та стійкості. Її роль у протидії гібридним загрозам виявляється у: підвищенні прозорості та підзвітності, адже цифрові платформи та відкриті дані сприяють більшій прозорості урядових рішень та фінансових потоків, що ускладнює корупційні схеми та підвищує довіру громадян; зміцненні кібербезпеки шляхом того, що впровадження сучасних протоколів безпеки, систем моніторингу загроз, навчання персоналу та використання хмарних технологій з високим ступенем захисту дозволяє ефективніше протистояти кібератакам; підвищенні стійкості критичної інфраструктури, коли цифрові рішення дозволяють забезпечити резервування даних, швидке відновлення систем після атак та дистанційне управління критичними об'єктами, що є життєво важливим; ефективній комунікації та протидії дезінформації, тому що цифрові канали дозволяють державі швидко та ефективно доносити достовірну інформацію до населення, спростовувати фейки та формувати позитивне сприйняття державної політики. В цьому контексті створення єдиних державних порталів інформації та використання штучного інтелекту для виявлення дезінформації є критично важливими; оптимізації управлінських процесів, цифровізація адміністративних процедур дозволяє прискорити прийняття рішень, зменшити бюрократію та підвищити оперативність реагування на кризи; також слід вказати на сприяння залученню громадян, адже електронні петиції, консультації та інтерактивні платформи дозволяють громадянам брати активну участь у формуванні державної політики, що зміцнює зв'язок між владою та суспільством [7].

Цифрова стійкість (digital resilience) – це багатогранне поняття, що охоплює здатність держави та суспільства функціонувати, адаптуватися та відновлюватися в умовах цифрових загроз, забезпечуючи при цьому безперебійність надання послуг та захист критичних функцій. Це стосується не лише технічного захисту даних, а й інституційної, соціальної та культурної сфер.

Основні підходи до розуміння концепту цифрової стійкості включають:

1. Технічний підхід: фокусується на здатності інформаційних систем витримувати атаки, відновлюватися після збоїв та забезпечувати безперебійність функціонування. Включає кібергігієну, резервне копіювання даних, системи виявлення вторгнень, шифрування та використання стійкої архітектури.

2. Інституційний підхід: акцентує увагу на наявності політики, законодавства, стратегій та процедур, які регулюють питання кібербезпеки, захисту даних та реагування на інциденти. Також включає співпрацю між державними органами, приватним сектором та міжнародними партнерами.

3. Організаційний підхід: стосується здатності організацій (державних установ, підприємств критичної інфраструктури) ефективно управляти кіберризиками, мати плани безперервності діяльності та відповідного реагування на інциденти, а також проводити навчання та підвищення кваліфікації персоналу.

4. Соціально-комунікаційний підхід: підкреслює важливість підвищення цифрової грамотності населення, формування критичного мислення для протидії дезінформації та побудови довіри між громадянами та державними інститутами у цифровому просторі. Наголошує, що стійке суспіль-

ство, здатне відрізняти правду від фейків, є ключовим елементом цифрової стійкості.

5. Комплексний (холістичний) підхід: об'єднує всі вищезгадані аспекти, розглядаючи цифрову стійкість як системну якість, що охоплює технологічні, людські, організаційні та правові виміри. Це інтегративний підхід, який визнає взаємозалежність усіх компонентів для забезпечення здатності держави функціонувати в умовах цифрових загроз [1].

Надзвичайно цінним для України є досвід країн, що активно впроваджують цифрові технології та стикаються з гібридними загрозами.

Одним з лідерів у сфері електронного урядування (e-governance) та кібербезпеки є Естонія. Її цифрова інфраструктура побудована на принципі X-Road – децентралізованої системи обміну даними між різними державними та приватними реєстрами, що забезпечує високу прозорість та безпеку. Країна активно розвиває електронне урядування, електронні вибори, цифрові ідентифікатори та забезпечує 99% державних послуг онлайн. За останні десятиріччя Естонія значно посилила свою кібербезпекову стратегію. Були створені Data Embassies – центри зберігання даних за межами країни, що гарантує безперервність функціонування навіть у разі знищення інфраструктури на території Естонії [6].

Одним з провідних світових центрів кібербезпеки та інновацій є Ізраїль. Країна інвестує значні кошти у кібербезпеку, має високорозвинений сектор кібертехнологій та налагоджену співпрацю між державним сектором, науковими установами та приватними компаніями. Завдяки наявності постійних загроз національній безпеці, Ізраїль розробив багаторівневу систему захисту, що включає проактивний моніторинг, системи раннього попередження, глибоку аналітику загроз та швидке реагування на інциденти. Акцент робиться на підготовці висококваліфікованих кадрів у галузі кібербезпеки та розвитку оборонних кібертехнологій.

Останнім часом активно розвиває цифровізацію державних послуг, впроваджуючи електронні ідентифікатори, електронний підпис та уніфіковані платформи для надання адміністративних послуг Литва. Країна приділяє значну увагу розвитку цифрових навичок населення. Активно зміцнює свій кіберзахист, інвестує в захист критичної інфраструктури та посилює співпрацю з партнерами по НАТО та ЄС у сфері обміну інформацією про кіберзагрози. Литва також активно протидіє дезінформації, розвиваючи медіаграмотність та підтримуючи незалежні ЗМІ [3].

Високим рівнем довіри до державних інститутів, що є важливою складовою стійкості держави відома Фінляндія. Країна активно впроваджує цифрові рішення у сфері освіти, охорони здоров'я та соціальних послуг, забезпечуючи високу якість життя громадян. Фінляндія робить акцент на комплексному підході до національної безпеки, що включає не лише військову, а й цивільну стійкість. Це передбачає підготовку населення до кризових ситуацій, забезпечення безперебійності функціонування критичної інфраструктури та активну протидію дезінформації. Країна інвестує у кіберзахист, але також фокусується на соціальній згуртованості та розвитку критичного мислення громадян.

Можливості адаптації зарубіжного досвіду впровадження цифрових технологій з метою протидії загрозам національним інтересам в українських реаліях полягають, на нашу думку, у наступному: архітектура X-Road може бути використана для побудови захищеної системи обміну даними між державними реєстрами України. Досвід Data Embassies є критично важливим для забезпечення безперервності функціонування державних систем. Надзвичайно актуальними є також розвиток державно-приватного партнерства у сфері кібербезпеки та акцент на підготовку висококваліфікованих фахівців; досвід проактивного захисту та швидкого реагування. Досвід Литви у протидії

Таблиця 1

Порівняльний аналіз зарубіжного досвіду впровадження цифрових технологій з метою протидії загрозам національним інтересам [4]

Критерій	Естонія	Ізраїль	Литва	Фінляндія
Ключовий фокус	Е-урядування, кібербезпека, децентралізація	Кіберінновації, оборонна кібербезпека	Цифрові послуги, кіберзахист, медіаграмотність	Комплексна безпека, соціальна стійкість
Головна особливість	X-Road, Data Embassies	Інвестиції в R&D, співпраця military-tech	Протидія дезінформації	Довіра до інститутів, підготовка населення
Основні виклики	Збереження лідерства, адаптація до нових загроз	Постійні зовнішні кібератаки, регіональна нестабільність	Гібридні загрози	Адаптація до стандартів НАТО

дезінформації та сприяння розвитку медіаграмотності є вкрай цінним для України. Також важливим є досвід захисту критичної інфраструктури від гібридних загроз. Комплексний підхід до національної стійкості, включаючи цивільну оборону та соціальну згуртованість, що демонструє Фінляндія, може бути імплементований в українській стратегії безпеки. Також слід звернути увагу на фінський досвід щодо зміцнення довіри до державних інститутів через прозорість та ефективність цифрових послуг [9].

Україна продемонструвала значні успіхи у цифровій трансформації, зокрема флагманським проєктом, який дозволив інтегрувати понад 100 державних послуг та документів в єдину цифрову екосистему, значно спрощуючи взаємодію громадян з державою є портал та застосунок «Дія». Він включає електронні документи (паспорт, водійські права, студентський квиток), електронні послуги (сплата податків, реєстрація бізнесу, отримання довідок) та функціонал для внутрішньо переміщених осіб. Останнім часом суттєво посилилася і цифрова стійкість українських державних реєстрів та критичної інфраструктури. Це було досягнуто завдяки швидкому перенесенню даних у хмарні сховища (як в Україні, так і за кордоном), посиленню кіберзахисту та міжнародній допомозі. Ініціативами, що значно підвищили прозорість державних закупівель та дозволили громадянському суспільству здійснювати моніторинг витрат бюджетних коштів є впровадження технології відкритих даних та електронних закупівель (ProZorro). Критично важливим для надання цифрових послуг був успішний розвиток цифрової інфраструктури, що дало змогу забезпечити доступу до інтернету в сільській місцевості, продовжувати розширення мережі 4G.

До основних викликів у сфері цифрової трансформації публічного управління для України можна віднести: по-перше дефіцит кваліфікованих кадрів, адже незважаючи на наявність талановитих фахівців, Україна все ще стикається з нестачею висококваліфікованих кібербезпекових експертів, розробників та менеджерів проєктів у сфері е-урядування; по-друге необхідність подальшого вдосконалення законодавства у сфері цифрового публічного управління, кібербезпеки та захисту персональних даних відповідно до європейських стандартів; по-третє, постійні та масштабні кібератаки, а також широке поширення дезінформації, вимагають подальшого зміцнення кіберзахисту та розвитку ефективних механізмів протидії ІПСО; по-четверте, незважаючи на досягнення, досі є актуальним завдання повної інтеграції безпекового виміру в усі аспекти цифрової трансформації, включаючи розробку та впровадження архітектури «безпека за замовчуванням» (security by design); по-п’яте, фінансові ресурси, адже потреба у значних інвестиціях для подальшого розвитку цифрової інфраструктури, кіберзахисту та навчання персоналу залишається актуальною; по-шосте, попри успіхи «Дії», важливо постійно працювати над збереженням та зміцненням довіри громадян до цифрових рішень та до влади в цілому, особливо в умовах гібридних впливів [10].

Для ефективної протидії поточним загрозам національним інтересам та зміцнення стійкості держави, Україні необхідно зосередитися на наступних напрямах:

1. Формування моделі цифрової стійкості, що включає:

− розробку комплексної стратегії цифрової стійкості, що має враховувати не лише технічні аспекти кібербезпеки, а й організаційні, правові, соціальні та комунікаційні компоненти. Вона повинна бути інтегрована у загальну Стратегію національної безпеки України;

− впровадження архітектури «security-by-design» в усі державні цифрові проєкти, це означає, що безпекові компоненти мають бути закладені в основу кожної нової системи чи послуги, а не додаватися постфактум;

− створення єдиної системи моніторингу та реагування на загрози, зокрема центри аналізу загроз, швидкого реагування та координації дій між різними відомствами;

− подальший розвиток гібридної інфраструктури, тобто забезпечення можливості перенесення критично важливих даних та систем у хмарні сховища, зокрема за кордон (наслідуючи досвід Естонії з Data Embassies), для підвищення стійкості до фізичного знищення;

− підвищення цифрової грамотності населення, передбачає розробку та реалізацію національних програм з медіаграмотності, критичного мислення та безпечної поведінки в інтернеті, що дозволить громадянам ефективніше розпізнавати дезінформацію та маніпуляції;

− вдосконалення системи захисту персональних даних шляхом забезпечення відповідності українського законодавства нормам GDPR та посилення відповідальності за порушення у сфері захисту даних.

2. Моніторинг ефективності цифрових рішень у протидії загрозам національним інтересам:

− розробка ключових показників ефективності для оцінки стійкості, що дозволить

об'єктивно оцінювати вплив цифрових рішень на зниження вразливості держави до гібридних загроз;

− регулярне проведення аудитів та перевірок державних інформаційних систем для виявлення вразливостей та їх усунення;

− створення системи зворотного зв'язку, формування механізмів для отримання відгуків від громадян та експертів щодо ефективності цифрових послуг та їх впливу на безпекову ситуацію;

− міжнародний бенчмаркінг, тобто постійний моніторинг та порівняння українських досягнень у сфері цифрової стійкості з найкращими міжнародними практиками [8].

3. Здійснення емпіричних досліджень впливу цифровізації на довіру до влади:

− проведення соціологічних досліджень шляхом регулярних опитувань громадської думки щодо рівня довіри до державних інститутів, сприйняття цифрових послуг та їх впливу на рівень безпеки;

− аналіз даних використання цифрових сервісів за допомогою вивчення статистики використання порталу та застосунку «Дія», кількості успішно наданих послуг, звернень громадян тощо, для виявлення кореляції з рівнем довіри;

− дослідження конкретних випадків успішного впровадження цифрових рішень та їх впливу на довіру, а також проведення інтерв'ю з представниками влади та громадянами з цього приводу;

− публікація результатів досліджень, що дозволить формувати об'єктивну картину та сприятиме подальшому вдосконаленню цифрової складової сфери публічного управління;

− залучення наукової спільноти та аналітичних центрів, активна співпраця з університетами, науковими установами та незалежними аналітичними центрами для проведення об'єктивних та незалежних досліджень.

Висновки. Цифрове публічне управління є невід'ємним елементом сучасної національної безпеки, особливо в контексті гібридних загроз. Україна продемонструвала значний прогрес у цифровій трансформації. Досвід Естонії, Ізраїлю, Литви та Фінляндії підтверджує, що ефективне цифрове врядування, інтегроване з потужною системою кібербезпеки та соціальною стійкістю, є ключовим для протидії зовнішнім та внутрішнім дестабілізуючим впливам.

Для подальшого зміцнення своєї стійкості, Україна має зосередитися на формуванні комплексної моделі цифрової стійкості, що включає технічні, інституційні та соціальні аспекти. Це передбачає не лише розвиток передових технологій кіберзахисту, але й підвищення цифрової грамотності населення, зміцнення довіри до державних інститутів через прозорість та ефективність цифрових послуг, а також поглиблення міжнародної співпраці. Постійний моніторинг ефективності впроваджених рішень та проведення емпіричних досліджень дозволять адаптувати стратегії та забезпечувати безперервний розвиток цифрового публічного управління як надійного щита від гібридних загроз.

Перспективними напрямами інтеграції безпекового виміру у цифрову трансформацію публічного управлівння в сучасних умовах є: «Security by Design» та «Privacy by Design», тобто інтеграція принципів безпеки та приватності на всіх етапах розробки та впровадження цифрових систем та послуг; пошук оптимального балансу між централізованим управлінням кібербезпекою та децентралізованими рішеннями для підвищення стійкості та зменшення ризиків єдиної точки відмови; поглиблення співпраці з міжнародними партнерами у сфері кібербезпеки, обмін розвідданими про загрози, спільні навчання та розробка стандартів; активна участь у міжнародних ініціативах з формування правил поведінки у кіберпросторі та протидії шкідливим кібероперація̈м; залучення приватного сектору до розвитку та захисту критичної інформаційної інфраструктури.

REFERENCES:

1. Bondarchuk, V. I. (2023). Tsyfrova transformatsiia derzhavnoho upravlinnia v konteksti natsionalnoi bezpeky Ukrainy [Digital transformation of public administration in the context of Ukraine's national security]. *Public Administration and Management*, *(1)*, 45–56.

2. Hrytsenko, A. M. (2022). Elektronne uriaduvannia yak instrument protydii hibrydnym zahrozam [E-governance as a tool to counter hybrid threats]. *Scientific Bulletin of Uzhhorod National University. Series: Law*, *(72)*, 2, 132–137.

3. Kovalenko, S. V. (2024). Kiberbezpeka v systemi publichnoho upravlinnia: vyklyky ta perspektyvy [Cybersecurity in the public administration system: Challenges and prospects]. *Public Administration: Theory and Practice*, *(2)*, 78–89.

4. Melnyk, O. P., & Prokopenko, L. O. (2023). Tsyfrova stiikist derzhavy: kontseptualni zasady ta instrumenty formuvannia [Digital resilience of the state: Conceptual foundations and formation tools]. *Bulletin of the National Academy of Public Administration under the President of Ukraine. Series: Public Administration*, *(3)*, 60–71.

5. Ponomarenko, Yu. V. (2022). Rol tsyfrovykh tekhnolohii u zabezpechenni informatsiinoi bezpeky ta protydii dezinformatsii [The role of digital technologies in ensuring information security and countering disinformation]. *Strategic Panorama*, *(4)*, 98–105.

6. Safronov, O. O., & Ivanov, P. R. (2021). Rozvytok elektronnoi demokratii yak chynnyk zmitsnennia natsionalnoi bezpeky [Development of e-democracy as a factor in strengthening national security].*Law and Security*, *(2)*, 45–50.

7. Tkachenko, V. A. (2024). Tsyfrovizatsiia publichnykh posluh yak element natsionalnoi stiikosti [Digitalization of public services as an element of national resilience]. *Bulletin of Taras Shevchenko National University of Kyiv. Series: Public Administration*, *(1)*, 34–42.

8. Shevchenko, M. S. (2023). Upravlinnia ryzykamy v tsyfrovii ekosystemi derzhavy: mizhnarodnyi dosvid ta ukrainski realii [Risk management in the digital ecosystem of the state: International experience and Ukrainian realities]. *Public Administration: Strategy and Tactics*, *(4)*, 23–34.

9. Yakovenko, L. I. (2022). Efektyvnist tsyfrovoho uriaduvannia v umovakh zovnishnikh zahroz [Effectiveness of digital governance under external threats]. *Scientific Works of Petro Mohyla Black Sea State University. Series: Public Administration*, *218*(206), 112–120.

10. International trends in e-governance for national security: A comparative analysis. (2021). *Journal of Public Administration and Governance*, *11*(3), 15–28.