ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 35:004:355.02

Алієв Азер Аріф огли
аспірант кафедри міжнародних відносин та політичного консалтингу
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
Aliyev Azer
Postgraduate Student of the International Relations and Political Consulting Department
"Ukraine" University
ORCID: 0009-0009-2040-1323

DOI: 10.25313/2520-2294-2025-11-11606

КОНЦЕПТУАЛЬНИЙ МЕХАНІЗМ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ ЯК ФАКТОР ГАРАНТУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

CONCEPTUAL MECHANISM OF DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION AS A FACTOR IN GUARANTEEING NATIONAL SECURITY

Анотація. *Вступ. Сучасні виклики глобалізації та технологічного розвитку створюють нові вимоги до ефективності державного управління та забезпечення національної безпеки. В даному контексті цифрова трансформація публічного управління виступає ключовим інструментом модернізації державних інституцій і підвищення їхньої стійкості до зовнішніх і внутрішніх загроз.*

Мета. Метою дослідження є розробка концептуального механізму цифрової трансформації публічного управління, здатного підвищити ефективність та прозорість державного управління, забезпечити інтеграцію цифрових технологій у державні процеси та гарантувати національну безпеку України в умовах сучасних внутрішніх і зовнішніх викликів.

Матеріали і методи. Матеріалами дослідження є: нормативно-правові акти України, що регламентують процеси цифрової трансформації, розвиток електронного урядування та забезпечення національної безпеки; стратегічні документи Європейського Союзу та міжнародних організацій, присвячені цифровізації публічного сектору та кібербезпеці; наукові праці вітчизняних і зарубіжних авторів, які досліджують проблематику цифрового управління, кіберзахисту та інституційної модернізації держави; аналітичні звіти провідних міжнародних експертних центрів та IT-компаній щодо впровадження цифрових технологій у публічному управлінні.

У процесі здійснення дослідження було використано такі наукові методи: системного аналізу (для визначення взаємозв'язків між цифровими технологіями, державними інституціями та безпековою сферою); структурно-функціонального підходу (для розкриття функціональних характеристик інституційного, організаційного та безпекового компонентів механізму цифрової трансформації); порівняльного аналізу (для оцінки досвіду цифровізації публічного управління у країнах ЄС та визначення релевантних практик для України); методу теоретичного узагальнення (для формування авторського концептуального механізму цифрової трансформації публічного управління); логічного моделювання (для побудови концептуальної схеми цифрової трансформації як фактора гарантування національної безпеки).

Результати. У статті обґрунтовано теоретико-методологічні засади цифрової трансформації публічного управління в контексті забезпечення національної безпеки. Цифровізація розглядається не лише як інструмент модернізації державного управління, але й як стратегічний чинник зміцнення стійкості держави до внутрішніх та зовнішніх викликів. Показано, що цифрові технології створюють нові можливості для підвищення ефективності управлінських процесів, прозорості діяльності органів влади, зміцнення довіри громадян до державних інституцій та протидії гібридним загрозам. Запропоновано концептуальний механізм цифрової трансформації публічного управління, який поєднує інституційний, нормативно-правовий, організаційний, технологічний та безпековий компоненти. Визначено, що його реалізація має ґрунтуватися на принципах відкритості, інтегрованості, інноваційності та кіберзахищеності. Особливу увагу приділено ролі кібербезпеки як ключового елемента забезпечення національної безпеки в умовах цифровізації. Наголошено, що

запропонований механізм сприяє підвищенню адаптивності та стійкості системи державного управління до глобальних викликів, таких як інформаційні війни, кібератаки, дезінформація та технологічна залежність. Водночас підкреслюється необхідність міжвідомчої координації, розвитку кадрового потенціалу та впровадження сучасних цифрових рішень для формування єдиного безпечного цифрового середовища держави.

Результати дослідження можуть бути використані у процесі розробки стратегічних документів цифрової трансформації, програм реформування публічного управління та державної політики у сфері національної безпеки. Запропонований концептуальний підхід створює підґрунтя для формування комплексної моделі цифрової держави, здатної ефективно реагувати на сучасні загрози та забезпечувати сталий розвиток України.

Перспективи. У подальших наукових дослідженнях доцільно зосередити увагу на розробці індикаторів оцінювання ефективності цифрової трансформації публічного управління в контексті національної безпеки, а також на визначенні рівня готовності державних інституцій до впровадження цифрових інновацій. Перспективним напрямом є дослідження взаємозв'язку між розвитком цифрової інфраструктури та підвищенням кіберстійкості держави, а також аналіз кадрового потенціалу у сфері цифрового управління.

Ключові слова: *механізм, цифрова трансформація, публічне управління, національна безпека, кібербезпека, цифрова держава.*

Summary. *Introduction. The modern challenges of globalization and technological development create new requirements for the effectiveness of public administration and national security. In this context, the digital transformation of public administration is a key tool for modernizing state institutions and increasing their resilience to external and internal threats.*

Purpose. The purpose of the study is to develop a conceptual mechanism for the digital transformation of public administration that can increase the efficiency and transparency of public administration, ensure the integration of digital technologies into public processes, and guarantee Ukraine's national security in the face of modern internal and external challenges.

Materials and methods. The research materials include: regulatory and legal acts of Ukraine governing the processes of digital transformation, the development of e-government, and national security; strategic documents of the European Union and international organizations devoted to the digitization of the public sector and cybersecurity; scientific works by domestic and foreign authors researching issues of digital governance, cyber security, and institutional modernization of the state; analytical reports by leading international expert centers and IT companies on the implementation of digital technologies in public administration.

The following scientific methods were used in the research process: system analysis (to determine the interrelationships between digital technologies, state institutions, and the security sphere); a structural-functional approach (to reveal the functional characteristics of the institutional, organizational, and security components of the digital transformation mechanism); comparative analysis (to assess the experience of digitalization of public administration in EU countries and identify relevant practices for Ukraine); theoretical generalization (to form the author's conceptual mechanism of digital transformation of public administration); logical modeling (to build a conceptual scheme of digital transformation as a factor in ensuring national security).

Results. The article substantiates the theoretical and methodological foundations of digital transformation of public administration in the context of ensuring national security. Digitalization is considered not only as a tool for modernizing public administration, but also as a strategic factor in strengthening the state's resilience to internal and external challenges. It is shown that digital technologies create new opportunities for improving the efficiency of management processes, the transparency of government activities, strengthening citizens' trust in state institutions, and countering hybrid threats. A conceptual mechanism for the digital transformation of public administration is proposed, combining institutional, regulatory, organizational, technological, and security components. It is determined that its implementation should be based on the principles of openness, integration, innovation, and cyber security. Particular attention is paid to the role of cybersecurity as a key element in ensuring national security in the context of digitalization. It is emphasized that the proposed mechanism contributes to increasing the adaptability and resilience of the public administration system to global challenges such as information warfare, cyberattacks, disinformation, and technological dependence. At the same time, the need for interagency coordination, human resource development, and the implementation of modern digital solutions to create a unified secure digital environment for the state is emphasized.

The results of the study can be used in the process of developing strategic documents for digital transformation, public administration reform programs, and state policy in the field of national security. The proposed conceptual approach creates the basis for the formation of a comprehensive model of a digital state capable of effectively responding to modern threats and ensuring the sustainable development of Ukraine.

Discussion. In further scientific research, it is advisable to focus on developing indicators for assessing the effectiveness of digital transformation of public administration in the context of national security, as well as determining the level of readiness of state institutions to implement digital innovations. A promising area of research is the study of the relationship between the development of digital infrastructure and the improvement of the state's cyber resilience, as well as the analysis of human resources in the field of digital governance.

Key words: *mechanism, digital transformation, public administration, national security, cybersecurity, digital state.*

Постановка проблеми. Сучасні держави стикаються зі значними викликами, пов'язаними зі швидким розвитком інформаційних та цифрових технологій, глобалізацією, зростанням кібератак і гібридних загроз. Україна, перебуваючи в умовах постійних політичних, економічних та безпекових викликів, потребує ефективних механізмів управління, здатних гарантувати стабільність та національну безпеку. Традиційні моделі публічного управління дедалі більше виявляють обмеженість у забезпеченні оперативності, прозорості та стійкості державних інституцій. Водночас цифровізація відкриває нові можливості для підвищення ефективності управлінських процесів, інтеграції міжвідомчих систем та своєчасного реагування на загрози національній безпеці. Проте відсутність чітко структурованого, концептуально обґрунтованого механізму цифрової трансформації публічного управління ускладнює системне впровадження інноваційних рішень та створює ризики для кібербезпеки та стійкості держави.

Таким чином, проблемою дослідження є розробка концептуального механізму цифрової трансформації публічного управління, який би забезпечував інтеграцію цифрових технологій у систему державного управління та гарантував національну безпеку в умовах сучасних викликів і загроз.

Аналіз останніх досліджень і публікацій. У наукових дослідженнях питання цифрової трансформації публічного управління та її значення для забезпечення національної безпеки отримало широке висвітлення. Зокрема дане питання, досліджували ряд вітчизняних та зарубіжних вчених.

Наприклад, Руденко Є. [1] зазначає, що розвиток інформаційних технологій формує основу мережевого суспільства, де цифрові інструменти стають ключовим чинником політичних і соціальних процесів. На думку, Губанової Н. [2] цифровізація відкриває нові можливості для розвитку електронного врядування, забезпечує прозорість діяльності органів влади та сприяє формуванню довіри громадян до державних інституцій. Медведенко І. [3] стверджує, що цифрова трансформація в Україні має розглядатися як стратегічний інструмент зміцнення державності, зокрема в контексті гібридних загроз. Чуба Н. [4] зазначає, що побудова цифрової держави неможлива без розвитку системи кіберзахисту, адже саме інформаційна безпека визначає стійкість країни до зовнішніх та внутрішніх викликів. Пташенко О. [5] підкреслює, що ефективність цифрових перетворень значною мірою залежить від кадрового забезпечення, готовності державних службовців до роботи в умовах цифрової екосистеми та наявності чіткої міжвідомчої координації.

Таким чином, аналіз останніх досліджень і публікацій дозволяє зробити висновок, що цифрова трансформація публічного управління розглядається науковцями та міжнародними інституціями як багатовимірний процес, який поєднує модернізацію управління, впровадження інноваційних технологій і забезпечення національної безпеки.

Метою статті є розробка концептуального механізму цифрової трансформації публічного управління, здатного підвищити ефективність та прозорість державного управління, забезпечити інтеграцію цифрових технологій у державні процеси та гарантувати національну безпеку України в умовах сучасних внутрішніх і зовнішніх викликів.

Матеріали і методи. Матеріалами дослідження є: нормативно-правові акти України, що регламентують процеси цифрової трансформації, розвиток електронного урядування та забезпечення національної безпеки; стратегічні документи Європейського Союзу та міжнародних організацій, присвячені цифровізації публічного сектору та кібербезпеці; наукові праці вітчизняних і зарубіжних авторів, які досліджують проблематику цифрового управління, кіберзахисту та інституційної модернізації держави; аналітичні звіти провідних міжнародних експертних центрів та IT-компаній щодо впровадження цифрових технологій у публічному управлінні.

У процесі здійснення дослідження було використано такі наукові методи: системного аналізу (для визначення взаємозв'язків між цифровими технологіями, державними інституціями та безпековою сферою); структурно-функціонального підходу (для розкриття функціональних характеристик інституційного, організаційного та безпекового компонентів механізму цифрової трансформації); порівняльного аналізу (для оцінки досвіду цифровізації публічного управління у країнах ЄС та визначення релевантних практик для України); методу теоретичного узагальнення (для формування авторського концептуального механізму цифрової трансформації публічного управління); логічного моделювання (для побудови концептуальної схеми цифрової трансформації як фактора гарантування національної безпеки).

Виклад основного матеріалу. У сучасних умовах стрімкого розвитку інформаційних технологій, глобалізації та зростання комплексних загроз безпеці держави публічне управління стає ключовим інструментом забезпечення національної стабільності. Цифрова трансформація державних інституцій не лише підвищує ефективність управлінських процесів, а й створює нові можливості для гарантування національної безпеки. Виклики, пов'язані з інформаційною безпекою, кіберзагрозами та гібридними впливами, вимагають від держави нових підходів до організації управлінських процесів. Саме тому цифрова трансформація розглядається не лише як інструмент модернізації державного сектору, але й як ключовий чинник забезпечення національної безпеки.

Теоретико-методологічні засади цифрової трансформації публічного управління в контексті національної безпеки ґрунтуються на кількох ключових підходах [6]:

– системний підхід — розглядає цифровізацію як комплексну зміну всієї системи публічного управління, де технології інтегруються у взаємодію держави, суспільства й бізнесу.
– інституційний підхід — пояснює роль державних органів та нормативно-правової бази у створенні цифрової інфраструктури, що здатна гарантувати безпеку даних та ефективність управління.
– безпековий підхід — акцентує на тому, що цифрові технології є не лише інструментом оптимізації, а й чинником протидії загрозам: кіберзлочинності, інформаційним атакам, гібридним викликам.
– гуманітарно-ціннісний підхід — підкреслює значення довіри громадян, прозорості державних процесів і захисту прав людини у цифровому середовищі.

Разом з тим, цифрова трансформація виступає не лише технічною модернізацією державного управління, а й стратегічним ресурсом зміцнення національної безпеки, підвищення стійкості держави до внутрішніх і зовнішніх викликів. Її стратегічне значення полягає у формуванні стійкості держави до широкого спектра внутрішніх та зовнішніх викликів. Адже, з одного боку, цифрові технології забезпечують прозорість та підзвітність управлінських рішень, сприяють боротьбі з корупцією та посилюють довіру громадян до інституцій влади. Таким чином, цифровізація виступає стратегічним чинником національної безпеки, адже вона формує адаптивну, гнучку й водночас захищену систему управління, здатну ефективно функціонувати навіть у кризових умовах [7].

Доцільно розглянути як цифрові технології впливають на публічне управління та національну безпеку (табл. 1).

Таким чином, цифровізація одночасно підвищує якість управління та зміцнює безпековий потенціал держави, поєднуючи зручність для громадян із захистом національних інтересів. Розробка концептуального механізму цифрової трансформації публічного управління має ключове значення, оскільки дозволяє поєднати різні елементи державної політики в єдину узгоджену систему. Вона забезпечує не лише технологічне оновлення управлінських процесів, а й створює основу для їхньої безпеки, прозорості та ефективності. Саме системність і комплексність підходу робить можливим перетворення цифровізації з окремих ініціатив на стратегічний інструмент зміцнення державності та національної безпеки (рис. 1).

Доцільно розглянути всі ключові елементи запропонованого механізму [12]:

1) **Інституційний компонент** — формування організаційної структури, відповідальної за цифрову трансформацію; визначення ролей державних органів, громадянського суспільства та бізнесу у процесі цифровізації.

2) **Нормативно-правовий компонент** — розробка законодавства та регуляторних актів, що забезпечують легітимність і безпеку цифрових процесів; створення стандартів для електронних послуг, захисту персональних даних та кібербезпеки.

3) **Організаційний компонент** — оптимізація управлінських процесів під цифрові формати; впровадження електронного документообігу, автоматизованих систем прийняття рішень і внутрішньої комунікації.

4) **Технологічний компонент** — впровадження сучасних IT-рішень: хмарних платформ, аналітики Big Data, штучного інтелекту; забезпечення сумісності цифрових систем і інтеграції між різними рівнями влади та галузями.

5) **Безпековий компонент** — розбудова кіберзахищеної інфраструктури, систем моніторингу та реагування на загрози; протидія гібридним атакам, забезпечення захисту персональних та державних даних.

6) **Принципи реалізації механізму — відкритість** — доступність інформації та послуг для громадян і бізнесу; прозорість прийняття рішень; інтегрованість — взаємодія усіх компонентів механізму та сумісність із наявними системами управління; інноваційність — впровадження сучасних технологій і нових методів управління; кіберзахищеність — пріоритет безпеки даних і стійкості державної цифрової інфраструктури.

Таблиця 1

Вплив цифрових технологій на ефективність управління, прозорість та національну безпеку

№	Можливість	Приклад впровадження	Результат
1	Підвищення ефективності управлінських процесів	Електронний документообіг, автоматизація послуг (e-government)	Швидше ухвалення рішень, зменшення бюрократії, економія ресурсів
2	Прозорість діяльності органів влади	Відкриті дані, електронні закупівлі, онлайн-декларації посадовців	Зниження корупції, контроль громадян за владою
3	Зміцнення довіри громадян до інституцій	Доступ до онлайн-сервісів, електронні петиції, публічні консультації	Підвищення довіри, активна участь громадян у прийнятті рішень
4	Протидія гібридним загрозам	Кібербезпекові системи, моніторинг інформаційного простору, захист критичної інфраструктури	Стійкість до кібератак, протидія дезінформації, координація дій у кризових умовах

Джерело: сформовано автором на основі даних [8]

Рис. 1. Концептуальний механізм цифрової трансформації публічного управління
Джерело: сформовано автором на основі даних [9–11]

Впровадження концептуального механізму цифрової трансформації публічного управління у практичну діяльність є необхідною умовою підвищення ефективності державного сектору та зміцнення національної безпеки. Такий механізм дозволяє забезпечити цілісність і узгодженість інституційних, нормативно-правових, організаційних, технологічних та безпекових складових, що формують єдину основу для модернізації управлінських процесів. Реалізація запропонованого механізму доцільна у поєднанні з упровадженням єдиної національної цифрової платформи, що інтегруватиме інституційні, технологічні та безпекові рішення, а також забезпечить залучення громадян до процесів прийняття управлінських рішень через інструменти е-демократії. Це дозволить зробити цифрову трансформацію не лише інструментом модернізації, а й ефективною моделлю сталого розвитку та захисту державності. Необхідною умовою ефективної реалізації механізму цифрової трансформації є міжвідомча координація, адже саме вона дозволяє узгодити діяльність різних органів влади, уникнути дублювання функцій і забезпечити єдині стандарти у сфері цифрового врядування. Не менш важливим є розвиток кадрового потенціалу, оскільки цифрова трансформація потребує фахівців із сучасними компетентностями у сфері інформаційних технологій, кібербезпеки та управління даними [13].

Разом з тим, концептуальний підхід до побудови цифрової держави має ґрунтуватися на інтеграції управлінських, технологічних і безпекових складових у єдину систему, що забезпечує ефективне функціонування держави у цифровому середовищі та її стійкість до сучасних викликів. Його сутність полягає у поєднанні трьох взаємопов'язаних вимірів [14]:

1) **Управлінський вимір —** побудова прозорої та підзвітної системи публічного управління; впровадження принципів е-демократії для посилення взаємодії з громадянами; забезпечення міжвідомчої координації та узгодженості цифрових політик.

2) **Технологічний вимір —** розбудова сучасної цифрової інфраструктури (хмарні рішення, Big Data, штучний інтелект, блокчейн); забезпечення сумісності та інтегрованості державних електронних сервісів; створення інноваційних платформ для тестування та впровадження нових технологій.

3) **Безпековий вимір —** формування єдиної системи кіберзахисту критичної інфраструктури; розвиток механізмів протидії дезінформації та гібридним загрозам; захист персональних даних і гарантування цифрових прав громадян.

Варто звернути увагу і на принципи реалізації підходу [15]: відкритість — прозорість державних процесів і доступність інформації для громадян; інтегрованість — єдність управлінських і технологічних рішень; інноваційність — постійне оновлення та використання новітніх технологій; кіберзахищеність — пріоритетна увага до захисту даних і цифрової інфраструктури.

Таким чином, запропонований концептуальний підхід створює підґрунтя для формування комплексної моделі цифрової держави, яка здатна не лише ефективно реагувати на сучасні загрози, а й забезпечувати сталий розвиток України шляхом підвищення ефективності управління, зміцнення національної безпеки та розширення можливостей громадян. Його практична реалізація дозволить вибудувати цілісну цифрову екосистему, у якій управлінські, технологічні та безпекові компоненти функціонуватимуть у взаємодії та взаємодоповненні.

Отже, цифрова держава, побудована на запропонованих засадах, постає не лише як відповідь на виклики сьогодення, а й як стратегічний інструмент модернізації країни, що формує нову якість публічного управління та забезпечує конкурентоспроможність України у глобальному цифровому просторі.

Зважаючи на визначену концептуальну основу цифрової трансформації публічного управління, доцільно виокремити низку практичних кроків, спрямованих на забезпечення її ефективної реалізації у вітчизняному контексті:

1) Розробити національну стратегію цифрової трансформації публічного управління, яка б поєднувала інституційні, правові, організаційні, технологічні та безпекові аспекти в єдину систему.

2) Створити єдину інтегровану цифрову платформу державних послуг, що забезпечить сумісність і взаємодію між усіма органами влади та унеможливить дублювання функцій.

3) Посилити міжвідомчу координацію, запровадивши механізми постійної взаємодії та обміну даними між центральними і місцевими органами влади.

4) Інвестувати у розвиток кадрового потенціалу, зокрема через системи підвищення кваліфікації та перепідготовки державних службовців у сфері цифрових технологій і кібербезпеки.

5) Запроваджувати сучасні цифрові рішення (Big Data, штучний інтелект, блокчейн, хмарні технології) для прогнозування ризиків, оптимізації управлінських процесів і підвищення прозорості.

6) Розбудувати комплексну систему кіберзахисту, яка включатиме моніторинг загроз, швидке реагування на кіберінциденти та міжнародне співробітництво у сфері безпеки.

7) Сприяти розвитку інструментів е-демократії, що забезпечать ширшу участь громадян у прийнятті державних рішень і підвищать рівень довіри до інституцій влади.

Запропоновані практичні рекомендації створюють цілісне підґрунтя для втілення концепції цифрової держави у практичну площину. Їх реалізація дозволить не лише оптимізувати діяльність органів влади, а й сформувати стійке, безпечне та інноваційне цифрове середовище, здатне зміцнити національну безпеку, підвищити ефективність управління та забезпечити активну участь громадян у розвитку України.

Висновки. Цифрова трансформація публічного управління виступає не лише інструментом модернізації державних інституцій, а й стратегічним чинником зміцнення національної безпеки та стійкості держави до внутрішніх і зовнішніх викликів. Запропонований концептуальний підхід та механізм, що поєднує інституційний, нормативно-правовий, організаційний, технологічний і безпековий компоненти, формують основу для побудови комплексної моделі цифрової держави. Реалізація цього підходу на засадах відкритості, інтегрованості, інноваційності та кіберзахищеності створює умови для підвищення ефективності управлінських процесів, забезпечення прозорості діяльності органів влади, розширення можливостей громадян, а також посилення спроможності України протидіяти сучасним загрозам.

Таким чином, цифрова держава має розглядатися як довгострокова стратегія розвитку країни, що поєднує управлінську ефективність, технологічний прогрес та національну безпеку, забезпечуючи при цьому сталий розвиток та конкурентоспроможність України у глобальному цифровому середовищі.

Література

1. Руденко Є., Шапран О., Махно Є. Цифрова трансформація як фактор покращення національної безпеки України. *Публічне управління та місцеве самоврядування.* 2024. № 2. С. 65–69. DOI: https://doi.org/10.32782/2414-4436/2024-2-9. URL: https://journals.politehnica.dp.ua/index.php/public/article/view/612 (дата звернення: 12.11.2025).

2. Косич М. В., Губанова Н. Н. Розвиток електронного урядування в Україні. *Вісник економіки транспорту і промисловості.* 2023. № 81–82. С. 52–59. DOI: https://doi.org/10.18664/btie.81-82.287126

3. Медведенко І. В. Електронне урядування: міжнародний досвід та перспективи для України. *Український економічний часопис.* 2024. № 6. С. 52–58. DOI: https://doi.org/10.32782/2786-8273/2024-6-9

4. Чуба Н. В. Електронне урядування та адаптація державної служби України до стандартів ЄС. *Публічне урядування.* 2022. № 2(30). С. 101–109. DOI: https://doi.org/10.32689/2617-2224-2022-2(30)-13

5. Птащенко О. В. Система соціальної безпеки міста в умовах цифрової трансформації. *Вісник Східноукраїнського національного університету імені В. Даля.* 2023. № 280–4. С. 41–46. DOI: https://doi.org/10.33216/1998-7927-2023-280-4-41-46

6. Арсенович Л. А. *Сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку*. Ефективність державного управління. 2024. № 68/69. С. 9–21. DOI: https://doi.org/10.36930/506801

7. Засуха М.В. Сутність цифрової трансформації публічного управління. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2024. № 12. DOI: https://doi.org/10.54929/2786-5746/2024-12-02-04

8. Данильян О.Г., Дзьобань О.Р., Білоусов Є.М., Калиновський Ю.Ю., Яковюк І.В. *Національна безпека у філософсько-правовому дискурсі: монографія*. Харків: ХНУПС, 2019. 244 с.

9. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 8. С. 28–35. DOI: https://doi.org/10.31470/2786-6246-2024-8-28-35

10. Харитонюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. *Економіка, управління та адміністрування.* 2021. № 3(97). С. 36–40. DOI: https://doi.org/10.26642/ema-2021-3(97)-36-40

11. Панченко О.А., Гнатенко В.С. *Економічна кібербезпека в державній системі національної безпеки*. *Публічне урядування.* 2021. № 2(27). С. 22–31. DOI: https://doi.org/10.32689/2617-2224-2021-2(27)-3

12. Біленець Д.А., Веселий В.С., Возняковська К.А., Волощук О.Т., Демчук Т.І., Латковська Т.А., Марчук В.В., Глиняний І.В., Факас І.Б., Цуркан-Сайфуліна Ю.В. Національна безпека України в реаліях масштабної військової агресії: колективна монографія. Чернівці, 2024. 550 с.

13. Пролоренzo А. Кібербезпека в українських літературних джерелах: політичний огляд. *Вісник Прикарпатського університету. Серія: Політологія.* 2025. № 20. С. 31–35. DOI: https://doi.org/10.32782/2312-1815/2025-20-4

14. Федорчак О., Пилипенко В., Буник Ю., Блинда Ю. Вплив електронного врядування на економічний розвиток України. *Financial and credit activity: problems of theory and practice.* 2024. Том 5, № 58. С. 390–407. DOI: https://doi.org/10.55643/fcaptp.5.58.2024.4494

15. Таран Є.І. Трансформація підходів до розуміння державної політики національної безпеки. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2025. № 1.12. DOI: https://doi.org/10.32782/tnv-pub.2025.1.12

References

1. Rudenko, Ye., Shapran, O., & Makhno, Ye. (2024). Tsyfrova transformatsiia yak faktor pokrashchennia natsionalnoi bezpeky Ukrainy [Digital transformation as a factor in improving Ukraine's national security]. *Publichne upravlinnia ta mistseve samovriaduvannia.* № 2. Pp. 65–69. DOI: https://doi.org/10.32782/2414-4436/2024-2-9. URL: https://journals.politehnica.dp.ua/index.php/public/article/view/612 [in Ukrainian].

2. Kosych, M.V., & Hubanova, N.N. (2023). Rozvytok elektronnoho uriaduvannia v Ukraini [Development of e-government in Ukraine]. *Visnyk ekonomiky transportu i promyslovosti.* № 81–82. Pp. 52–59. DOI: https://doi.org/10.18664/btie.81-82.287126. [in Ukrainian].

3. Medvedenko, I.V. (2024). Elektronne uriaduvannia: mizhnarodnyi dosvid ta perspektyvy dlia Ukrainy [E-government: International experience and prospects for Ukraine]. *Ukrainskyi ekonomichnyi chasopys.* № 6. Pp. 52–58. DOI: https://doi.org/10.32782/2786-8273/2024-6-9 [in Ukrainian].

4. Chuba, N.V. (2022). Elektronne uriaduvannia ta adaptatsiia derzhavnoi sluzhby Ukrainy do standartiv YeS [E-government and adaptation of Ukraine's civil service to EU standards]. *Publichne uriaduvannia.* № 2(30). Pp. 101–109. DOI: https://doi.org/10.32689/2617-2224-2022-2(30)-13 [in Ukrainian].

5. Ptashchenko, O.V. (2023). Systema sotsialnoi bezpeky mista v umovakh tsyfrovoi transformatsii [Urban social security system under digital transformation]. *Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni V. Dalia.* № 280–4. Pp. 41–46. DOI: https://doi.org/10.33216/1998-7927-2023-280-4-41-46 [in Ukrainian].

6. Arsenovych, L.A. (2024). Sutnist kiberbezpeky yak napriamu vyroblennia derzhavnoi polityky tsyfrovoho rozvytku [The essence of cybersecurity as a direction of forming the state policy of digital development]. *Efektyvnist derzhavnoho upravlinnia.* № 68/69. Pp. 9–21. DOI: https://doi.org/10.36930/506801 [in Ukrainian].

7. Zasukha, M.V. (2024). Sutnist tsyfrovoi transformatsii publichnoho upravlinnia [The essence of digital transformation of public administration]. *Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia.* № 12. DOI: https://doi.org/10.54929/2786-5746/2024-12-02-04 [in Ukrainian].

8. Danylyan, O.H., Dzoban, O.R., Bilousov, Ye.M., Kalynovskyi, Yu.Yu., Yakoviuk, I.V., & others. (2019). Natsionalna bezpeka u filosofsko-pravovomu dyskursi [National security in philosophical and legal discourse]. Kharkiv: KhNUP S. 244 p. [in Ukrainian].

9. Vovk, A. (2024). Suchasni problemy publichnoho upravlinnia zabezpechenniam kiberbezpeky v Ukraini [Modern problems of public administration in ensuring cybersecurity in Ukraine]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia.* № 8. Pp. 28–35. DOI: https://doi.org/10.31470/2786-6246-2024-8-28-35 [in Ukrainian].

10. Kharytoniuk, K.Kh. (2021). Mekhanizmy derzhavnoho upravlinnia kiber- ta informatsiinoiu bezpekoiu: problemy ta shliakhy vyrishennia [Mechanisms of public administration of cyber and information security: problems and solutions]. *Ekonomika, upravlinnia ta administruvannia.* № 3(97). 36–40. DOI: https://doi.org/10.26642/ema-2021-3(97)-36-40 [in Ukrainian].

11. Panchenko, O.A., & Hnatenko, V.S. (2021). Ekonomichna kiberbezpeka v derzhavnii systemi natsionalnoi bezpeky [Economic cybersecurity in the state system of national security]. *Publichne uriaduvannia.* 2(27). Pp. 22–31. DOI: https://doi.org/10.32689/2617-2224-2021-2(27)-3 [in Ukrainian].

12. Bilents, D.A., Veselyi, V.S., Vozniakovska, K.A., Voloshchuk, O.T., Demchuk, T.I., & others. (2024). Natsionalna bezpeka Ukrainy v realiiakh masshtabnoi viiskovoi ahresii [National security of Ukraine under large-scale military aggression]: Collective monograph. Chernivtsi. 550 p. [in Ukrainian].

13. Prolorenzo, A. (2025). Kiberbezpeka v ukrainskykh literaturnykh dzherelakh: politychnyi ohliad [Cybersecurity in Ukrainian literary sources: A political review]. *Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia.* (20). Pp. 31–35. DOI: https://doi.org/10.32782/2312-1815/2025-20-4 [in Ukrainian].

14. Fedorchak, O., Pylypenko, V., Bunyk, Yu., Blynda, Yu., & others. (2024). Vplyv elektronnoho vriaduvannia na ekonomichnyi rozvytok Ukrainy [The impact of e-governance on Ukraine's economic development]. *Financial and credit activity: problems of theory and practice.* № 5(58). Pp. 390–407. DOI: https://doi.org/10.55643/fcaptp.5.58.2024.4494

15. Taran, Ye.I. (2025). Transformatsiia pidkhodiv do rozuminnia derzhavnoi polityky natsionalnoi bezpeky [Transformation of approaches to understanding national security policy]. *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia.* № (1.12). DOI: https://doi.org/10.32782/tnv-pub.2025.1.12 [in Ukrainian].