ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

УДК 351.746

DOI: https://doi.org/10.32782/2708-0366/2025.25.18

Алієв А.А.
аспірант,
Заклад вищої освіти «Відкритий міжнародний університет
розвитку людини «Україна»
ORCID: https://orcid.org/0009-0009-2040-1323

Aliyev Azer
Higher Education Institution "Open International University of
Human Development "Ukraine"

ЦИФРОВІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: СВІТОВІ ТЕНДЕНЦІЇ ТА РЕКОМЕНДАЦІЇ ДЛЯ УКРАЇНИ

DIGITALIZATION OF PUBLIC ADMINISTRATION IN THE SPHERE OF NATIONAL SECURITY: GLOBAL TRENDS AND RECOMMENDATIONS FOR UKRAINE

У статті здійснено аналіз глобальних тенденцій цифровізації публічного управління у сфері безпеки, включаючи впровадження інтелектуальних інформаційних систем, штучного інтелекту, кіберзахисту, хмарних технологій та інтегрованих платформ для прийняття рішень в умовах криз. Розглянуто досвід провідних країн, таких як США, Естонія, Ізраїль, Канада, Велика Британія, Фінляндія, Австралія, Німеччина і т.д., а також нормативно-правові підходи Європейського Союзу до цифрової безпеки та управління ризиками. Визначено ключові виклики, що стримують процес цифровізації, серед яких – фрагментарність цифрової інфраструктури, низька інтеграція інформаційних систем, брак кадрів та нормативна неврегульованість. Запропоновано стратегічні рекомендації щодо вдосконалення цифрового управління в Україні, що включають розвиток кіберкомандних структур, посилення міжвідомчої взаємодії, впровадження національних стандартів цифрової безпеки та створення єдиної платформи для управління ризиками в умовах надзвичайних ситуацій. Дослідження має практичне значення для формування державної політики у сфері цифрової трансформації безпекового сектору та спрямоване на посилення стійкості України до сучасних загроз.

Ключові слова: *цифровізація, публічне управління, національна безпека, економічний розвиток, цифрова трансформація, кібербезпека.*

Digitalization of public administration in the field of national security is one of the key trends in modern state development. In the context of growing cyber threats, hybrid challenges, and global instability, countries around the world are actively implementing digital technologies to improve the efficiency, transparency, and effectiveness of their security systems. For Ukraine, which is in a state of armed aggression and at the same time seeks to integrate into the European and Euro-Atlantic security space, adaptation to global practices of digital governance in this area is extremely relevant. This requires not only technical modernization, but also deep institutional reforms and the development of national recommendations based on global experience. At the same time, in today's environment, digital transformation covers all areas of public administration,

including the national security sector, which requires special attention given the growing threats, hybrid challenges and high level of instability in the world. The article analyzes global trends in the digitalization of public administration in the security sector, including the introduction of intelligent information systems, artificial intelligence, cyber defense, cloud technologies and integrated decision-making platforms in crises. The experience of leading countries, such as the United States, Estonia, Israel, Canada, the United Kingdom, Finland, Australia, Germany, etc., as well as the regulatory approaches of the European Union to digital security and risk management are considered. Particular attention is paid to the current state of digital transformation in the national security system of Ukraine in the context of war and post-war reconstruction. The key challenges that hinder the digitalization process are identified, including the fragmentation of digital infrastructure, low integration of information systems, lack of personnel and regulatory uncertainty. The author proposes strategic recommendations for improving digital governance in Ukraine, including the development of cyber command structures, strengthening interagency cooperation, implementing national digital security standards, and creating a single platform for risk management in emergency situations. The study is of practical importance for the formation of state policy in the field of digital transformation of the security sector and is aimed at strengthening Ukraine's resilience to modern threats.

Keywords: *digitalization, public administration, national security, economic development, digital transformation, cybersecurity.*

Постановка проблеми. У сучасному світі національна безпека дедалі більше залежить від здатності держав ефективно інтегрувати цифрові технології в систему публічного управління. Зростання кіберзагроз, гібридних війн, інформаційних атак та технологічних ризиків вимагає від урядів нових підходів до управління безпековими процесами, зокрема через впровадження інноваційних цифрових рішень. Світова практика демонструє позитивний досвід застосування цифрових інструментів для підвищення стійкості держав, оперативного реагування на загрози та забезпечення координації між інституціями безпеки. Водночас, в Україні цифровізація публічного управління в секторі національної безпеки залишається фрагментарною, слабо інтегрованою та обмеженою у нормативному та інституційному вимірах, що знижує ефективність управлінських рішень у кризових ситуаціях, зокрема в умовах збройної агресії.

У зв'язку з цим постає необхідність системного аналізу міжнародного досвіду цифрової трансформації безпекового управління, виявлення чинників, що сприяють або перешкоджають цьому процесу, та розробки практичних рекомендацій для вдосконалення відповідної політики в Україні. Актуальність проблеми зумовлена як безпековими викликами, так і прагненням держави до євроатлантичної інтеграції, що передбачає гармонізацію цифрової інфраструктури у сфері національної безпеки з міжнародними стандартами.

Аналіз останніх досліджень і публікацій. Цифровізація публічного управління у сфері національної безпеки набуває дедалі більшого значення в умовах глобальних викликів, і сучасні наукові дослідження відображають різноманітні підходи, моделі та практики впровадження цифрових технологій у цій сфері, що формують підґрунтя для розробки ефективних рекомендацій для України. Доцільно розглянути позиції вітчизняних та зарубіжних вчених щодо цієї проблеми.

Наприклад, на думку, Новікової Н. Л. зазначає, що цифровізація національної безпеки передбачає не лише впровадження ІКТ у публічне управління, а й комплексну трансформацію управлінських процесів у кризових умовах, зокрема в умовах війни та надзвичайних ситуацій [1]. Пігарєв Ю. В. вважає, що діджиталізація публічного управління є ключовим чинником підвищення прозорості, ефективності та оперативності державного реагування на новітні загрози, у тому числі кібернетичного характеру [2]. Саприкін В. В. звертає увагу на фрагментарність цифрової інфраструктури в Україні, що ускладнює процес інтеграції цифрових рішень у сфері національної безпеки, знижуючи загальну ефективність державного управління [3]. Особливої уваги заслуговує дослідження Margaret C. Hardy, адже він зазначає, що цифрова трансформація безпекових інституцій повинна відбуватися з урахуванням демократичних

стандартів, прозорості рішень та захисту громадянських прав, що особливо важливо у контексті впровадження технологій штучного інтелекту в державному секторі [4]. David J. Gerstein стверджує, що цифрова стійкість держав залежить від здатності урядів координувати багаторівневу політику кібербезпеки, зокрема через створення міжінституційних платформ та обов'язкових протоколів обміну інформацією між секторами [5]. Agnes Hubert наголошує на важливості впровадження єдиних стандартів кіберзахисту в межах ЄС, посилаючись на позитивний досвід застосування Директиви NIS2, що охоплює широкий спектр критичних інфраструктур, від енергетики до цифрових платформ [6].

Отже, аналіз наукових підходів свідчить про зростаючий інтерес до проблематики цифровізації публічного управління у сфері національної безпеки як в українському, так і в міжнародному академічному дискурсі. Водночас, більшість досліджень зосереджені або на загальних аспектах цифрової трансформації, або на окремих компонентах кібербезпеки, залишаючи поза увагою цілісне бачення системної цифровізації саме у сфері безпекового публічного управління в умовах сучасних викликів.

Формулювання цілей статті. Мета статті полягає в аналізові світових тенденцій цифровізації публічного управління у сфері національної безпеки, виявленні ключових технологічних та управлінських практик, а також розробленні рекомендацій щодо їх адаптації та впровадження в Україні з урахуванням сучасних викликів безпеки та стратегічного курсу на євроатлантичну інтеграцію.

Виклад основного матеріалу. У XXI столітті цифровізація стала визначальним чинником трансформації публічного управління, особливо у таких критично важливих сферах, як національна безпека. В умовах зростання гібридних загроз, кібератак та інформаційних війн, уряди по всьому світу активно впроваджують цифрові технології для підвищення ефективності, координації та оперативності управлінських рішень. Цей процес супроводжується створенням нових інституційних моделей, нормативно-правових механізмів і технічних рішень, які спрямовані на забезпечення безпеки держави в умовах цифрової доби. Для України, що перебуває у стані тривалої збройної агресії з боку Російської Федерації, питання цифрового реформування системи національної безпеки набуває особливої актуальності. Необхідність вивчення й адаптації кращих міжнародних практик зумовлює потребу у комплексному дослідженні глобальних тенденцій цифровізації та їх потенційного застосування в українських реаліях.

Публічне управління в цій сфері зазнає глибоких змін під впливом новітніх технологій, які суттєво змінюють як процеси стратегічного планування, так і оперативного реагування на загрози. Глобальні тенденції цифровізації у сфері безпеки охоплюють кілька взаємопов'язаних напрямів, які доцільно розглянути більш детально: інтелектуальні інформаційні системи, штучний інтелект (ШІ), кібербезпека, хмарні технології, інтегровані цифрові платформи для кризового управління [7].

Загальносвітові тенденції цифровізації публічного управління у сфері безпеки свідчать про перехід від фрагментарних цифрових рішень до системної трансформації державного управління із залученням високих технологій. Такий підхід не лише підвищує ефективність роботи безпекових структур, а й формує нову культуру управління ризиками та кризами. Для України вивчення й адаптація цих практик є особливо важливими в умовах збройного конфлікту та необхідності посилення державної стійкості на всіх рівнях (табл. 1).

В наслідок цього, міжнародний досвід демонструє, що цифровізація безпекового управління – це не лише технологічний виклик, а й стратегічна необхідність для сучасної держави. Країни, що досягли успіху в цій сфері, об'єднують цифрові інструменти з гнучкими управлінськими підходами, правовими рамками та міжвідомчою координацією. Для України, яка стикається із загрозами прямої військової агресії, інформаційного впливу та кібератак, імплементація подібних моделей має критичне значення.

Таблиця 1

Глобальні тенденції цифровізації публічного управління у сфері безпеки (приклади)

№	Тенденції цифровізації публічного управління	Досвід провідних країн щодо цифровізації публічного управління у сфері безпеки
1.	Інтелектуальні інформаційні системи	США: У Сполучених Штатах діє система DHS HSIN (Homeland Security Information Network), яка забезпечує обмін інформацією між федеральними, регіональними та місцевими органами у сфері безпеки. Вона дозволяє у режимі реального часу передавати дані, координувати дії підрозділів і забезпечувати реагування на загрози, у тому числі терористичні та природні катастрофи. Ізраїль: Ізраїль має інтегровану систему національного спостереження та аналітики, що об'єднує дані з камер спостереження, сенсорів, дронів та систем кібермоніторингу. Ці інструменти допомагають ефективно запобігати атакам та забезпечувати безпеку критичної інфраструктури.
2.	Штучний інтелект (ШІ)	Велика Британія: У 2021 році уряд запровадив програму використання ШІ в національній поліції (National Data Analytics Solution), яка застосовується для прогнозування злочинності, ідентифікації потенційно небезпечних осіб та управління безпековими інцидентами. Канада: Міністерство національної оборони Канади використовує алгоритми ШІ для аналізу супутникових знімків, розвідданих та прогнозування рухів потенційних противників у зоні конфліктів, зокрема у рамках програм NATO.
3.	Кібербезпека	Естонія: Після масштабної кібератаки у 2007 році Естонія стала лідером у галузі кіберзахисту. Було створено Центр кіберзахисту НАТО (CCDCOE) у Таллінні, а система e-Government працює на базі децентралізованої інфраструктури з багаторівневою системою кіберзахисту. Фінляндія: Створила національну агенцію кібербезпеки Traficom, яка координує захист цифрової інфраструктури, співпрацює з приватним сектором і впроваджує принципи кіберстійкості як обов'язкові елементи національного планування безпеки.
4.	Хмарні технології	Сінгапур: Ініціатива "Smart Nation" включає повномасштабне впровадження хмарних рішень у державному секторі, зокрема в управлінні безпековими службами. Хмарні платформи забезпечують швидкий доступ до даних, аналітику у реальному часі та стійкість до збоїв. Естонія: Використовує концепцію "Data Embassy", за якою державні дані зберігаються в хмарному середовищі за кордоном (наприклад, у Люксембурзі), що дозволяє продовжити функціонування держави навіть у разі окупації або фізичного знищення серверів на території країни.
5.	Інтегровані платформи для кризового управління	Німеччина: Національний центр управління кризовими ситуаціями (GMLZ) об'єднує цифрові канали комунікації між федеральними міністерствами, поліцією, службами медицини, пожежною охороною та армією. Він використовує цифрові платформи для координації дій у випадках терактів, катастроф або пандемій. Австралія: Система Emergency Management Australia (EMA) функціонує як цифрова платформа координації всіх ланок реагування під час надзвичайних ситуацій. EMA інтегрує дані від служб надзвичайного реагування, метеослужб, армії та поліції, забезпечуючи єдиний інформаційний простір.

Джерело: сформовано автором на основі даних [8–10]

Вивчення досвіду Естонії, Ізраїлю, Сінгапуру, США та інших країн може стати основою для формування національної стратегії цифрової трансформації системи безпеки.

З огляду на вищезазначене та з урахуванням світових технологічних зрушень, особливо у сфері штучного інтелекту та кібербезпеки, ключовим стає питання нормативного забезпечення цифрової трансформації. Найбільш послідовну і системну модель такого підходу демонструє Європейський Союз, що заслуговує на детальний аналіз.

Європейський Союз (ЄС) послідовно формує комплексну нормативно-правову базу у сфері цифрової безпеки, спрямовану на захист критичної інфраструктури, забезпечення кіберстійкості, ефективне управління ризиками та узгодження дій держав-членів. Регулювання цифрової безпеки в ЄС ґрунтується на поєднанні стратегічних документів, директив, регламентів, рекомендацій та міжінституційної координації, розглянемо це більш детальніше:

1. Директива NIS (Network and Information Security Directive) (2016/1148/EU) [11] – перший нормативно-правовий акт ЄС, що встановлює мінімальні вимоги до кібербезпеки для операторів критично важливої інфраструктури (енергетика, транспорт, фінанси, охорона здоров'я, цифрові послуги тощо). Оновлення – Директива NIS2 [12] (2022/2555/EU): розширення сфери дії на більшу кількість суб'єктів; посилення вимог до управління ризиками, аудиту безпеки та звітності; введення механізмів контролю і санкцій за порушення.

2. Європейський акт про кіберстійкість (EU Cyber Resilience Act, 2023) [13] – цей регламент спрямований на встановлення єдиних вимог до кібербезпеки для всіх цифрових продуктів і програмного забезпечення на ринку ЄС.

3. Акт про кібербезпеку (EU Cybersecurity Act, 2019) [14] – регламент (EU) 2019/881 зміцнює роль Агентства ЄС з кібербезпеки (ENISA), надаючи їй повноваження щодо: координації міждержавної політики; розробки загальноєвропейських сертифікаційних схем; підтримки держав-членів у випадку кіберінцидентів.

4. Регламент DORA (Digital Operational Resilience Act, 2022) [15] – встановлює вимоги до операційної цифрової стійкості у фінансовому секторі ЄС: управління IT-ризиками; оцінку цифрової загрозостійкості; механізми тестування (penetration testing); регулювання взаємодії з IT-постачальниками.

5. Європейська стратегія кібербезпеки (2020–2025) [16] – це ключовий стратегічний документ, що визначає довгострокові пріоритети ЄС: забезпечення цифрового суверенітету; посилення стійкості критичної інфраструктури; побудова єдиного європейського кіберпростору; розширення співпраці з НАТО, ООН та іншими партнерами.

6. Механізм управління ризиками [17]. Європейський Союз впроваджує системний підхід до управління цифровими ризиками, орієнтуючись на ранню ідентифікацію загроз, мінімізацію вразливостей та посилення цифрової стійкості як державних, так і приватних суб'єктів.

7. Міжінституційна та міжнародна координація [18]. Однією з сильних сторін підходу ЄС є розвиток інституційної мережі співпраці між державами-членами, агентствами ЄС, приватним сектором і міжнародними партнерами. Така координація забезпечує не лише обмін інформацією, а й єдине стратегічне бачення цифрової безпеки.

Ключові інституційні елементи: ENISA (Агентство ЄС з кібербезпеки); мережа CSIRTs; EU-CyCLONe (European Cyber Crisis Liaison Organisation Network); Європейська рада з цифрових ризиків (Digital Resilience Board) [19].

Як результат, нормативно-правова система ЄС у сфері цифрової безпеки поступово переходить від фрагментарного регулювання до інтегрованої моделі, що охоплює інфраструктуру, продукти, послуги, ризики та міжнародну співпрацю. Особливу увагу приділено стандартизації, кіберстійкості, сертифікації безпеки та відповідальності учасників цифрового ринку. Цей досвід є надзвичайно цінним для України, яка прагне гармонізувати своє законодавство з європейським і потребує комплексної моделі управління цифровими ризиками в умовах війни та післявоєнного відновлення [20].

Як результат дослідження, доцільно визначити ключові виклики, що стримують процес цифровізації публічного управління у сфері національної безпеки України, які особливо загострилися в умовах війни та потребують комплексного подолання як у коротко-, так і в довгостроковій перспективі.

Серед головних бар'єрів виокремлено:

1. Фрагментарність цифрової інфраструктури, яка проявляється у відсутності єдиного архітектурного підходу до цифровізації державних органів, нерівномірному розвитку ІТ-рішень у міністерствах і регіонах, а також наявності застарілих або незахищених систем у сфері безпеки та оборони.

2. Низький рівень інтеграції інформаційних систем, що ускладнює оперативний обмін даними між відомствами, гальмує процес прийняття управлінських рішень у кризових умовах та створює ризики дублювання функцій або втрати важливої інформації.

3. Брак висококваліфікованих ІТ-кадрів, особливо в регіональних структурах безпеки, правоохоронних органах та підрозділах цивільного захисту. Війна спричинила як фізичне знищення частини потенціалу, так і трудову міграцію спеціалістів у приватний або закордонний сектор.

4. Нормативна неврегульованість цифрових процесів, яка стосується як захисту персональних даних, так і процедур використання хмарних технологій, електронної ідентифікації, обміну інформацією в реальному часі тощо. Наявна правова база часто відстає від швидких технологічних змін або є фрагментарною та декларативною.

У відповідь на ці виклики варто запропонувати стратегічні рекомендації, що мають на меті формування сталого, адаптивного та безпечного цифрового середовища в секторі національної безпеки:

1. Розвиток кіберкомандних структур на базі ЗСУ, СБУ, Держспецзв'язку та інших відомств, здатних здійснювати активну кібероборону, аналіз загроз, і оперативну координацію дій на національному та міжнародному рівнях. Особливо важливим є забезпечення їхніх кадрових, технологічних та аналітичних спроможностей.

2. Посилення міжвідомчої взаємодії через створення інтегрованих цифрових платформ для спільного аналізу ризиків, обміну оперативною інформацією та координації рішень. Це включає впровадження спільних протоколів, централізованих баз даних та автоматизованих систем попередження кризових ситуацій.

3. Запровадження національних стандартів цифрової безпеки, гармонізованих з вимогами ЄС (зокрема, на основі директиви NIS2), які мають регламентувати технічні, процедурні та етичні аспекти використання цифрових технологій у секторі безпеки. Це передбачає також створення системи сертифікації та аудитів.

4. Формування єдиної платформи управління ризиками в умовах надзвичайних ситуацій, яка об'єднає цифрові інструменти прогнозування, реагування та координації на основі штучного інтелекту, хмарних технологій та геоінформаційних систем. Така платформа має слугувати спільним інструментом для Ситуаційного центру РНБО, ДСНС, МОУ та інших органів.

5. Інвестування в цифрову освіту та підготовку кадрів, включаючи створення спеціалізованих програм у вишах, підвищення кваліфікації державних службовців і розвиток публічно-приватного партнерства у сфері кіберосвіти.

6. Цифрова трансформація у процесі відновлення – використання цифрових інструментів у системах контролю реконструкції, прозорості гуманітарних поставок, обліку втрат та управління ресурсами в умовах поствоєнного відновлення.

Узагальнюючи викладене, можна стверджувати, що цифрова трансформація публічного управління у сфері національної безпеки є визначальним чинником стійкості держави в умовах сучасних загроз. Впровадження інтегрованих цифрових рішень, зміцнення нормативно-правової бази та розвиток кіберкомандних структур мають стати стратегічними пріоритетами політики безпеки України в умовах війни та в процесі післявоєнного відновлення.

Висновки. У контексті триваючої агресії Російської Федерації та гібридного характеру викликів, з якими стикається Україна, цифровізація публічного управління у сфері безпеки стає не просто інноваційним трендом, а нагальною державною потребою. Запропоновані у дослідженні аналітичні висновки та стратегічні рекомендації мають прикладний характер і можуть бути використані як основа для: оновлення нормативно-правової бази з урахуванням стандартів ЄС (зокрема NIS2, DORA, GDPR), що сприятиме гармонізації української політики цифрової безпеки з європейськими підходами – ключовий крок на шляху євроінтеграції; розробки національних програм і стратегій у сфері цифрової трансформації сектору безпеки, включаючи впровадження стандартів кіберзахисту, інтеграцію інформаційних систем та створення централізованих платформ управління ризиками; побудови адаптивної архітектури цифрової стійкості, яка дозволить ефективно реагувати на кризові ситуації, зокрема за допомогою інтелектуального аналізу даних, прогнозних моделей загроз і автоматизованого управління інцидентами; оптимізації міжвідомчої взаєм одії в режимі реального часу – через створення єдиних цифрових екосистем для СБУ, РНБО, ДСНС, Міноборони, Мінцифри та інших структур, що підвищить швидкість і точність ухвалення управлінських рішень у сфері національної безпеки; вдосконалення системи професійної підготовки ІТ-фахівців у сфері безпеки, розширення публічно-приватного партнерства у розробці безпекових цифрових рішень та залучення міжнародного досвіду до національних програм.

Таким чином, результати дослідження можуть бути застосовані як на рівні формування конкретних політичних ініціатив, так і для оперативного удосконалення функціонування існуючих інституцій, що прямо впливає на загальнонаціональну спроможність України протидіяти сучасним кіберзагрозам, дестабілізаційним кампаніям і ризикам у сфері критичної інфраструктури. З огляду на післявоєнну відбудову, ці напрацювання також мають стратегічну довготривалу вартість для побудови цифрової держави нового покоління.

Список використаних джерел:

1. Новікова Н. Л., Бойко Л. В. Цифровізація та національна безпека: тенденції та виклики. *Національна безпека: право та економіка.* 2024. № 1. С. 15–28. DOI: http://doi.org/10.51369/3083-5917-2024-1-8 (дата звернення 12.09.2025).

2. Пігарєв Ю., Костенюк Н. Діджиталізація публічного управління як чинник цифрової трансформації України. *Актуальні проблеми держуправління.* 2023. С. 23–34.

3. Саприкін В. Оцифровування, цифровізація та цифрова трансформація публічного управління в Україні. *Вісник КНУ імені Т. Шевченка. Серія: Державне управління.* 2024. Т. 19, № 1. С. 116–121. DOI: https://doi.org/10.17721/2616-9193.2024/19-19/22

4. Hardy M. C. Digital transformation of security institutions: Between technology and democratic values. J*ournal of Public Security Innovation.* 2022. Vol. 15, No. 2. C. 45–59.

5. Gerstein D. J. Building digital resilience: New challenges to national security. *Cybersecurity & Policy Review.* 2021. Vol. 9, No. 1. C. 21–38.

6. Hubert A. European cybersecurity policy: Implementation of the NIS2 Directive. *European Security Studies.* 2023. Vol. 18, No. 3. C. 64–77.

7. Руденко Є., Шапран О., Махно Є. Цифрова трансформація як фактор покращення національної безпеки України. *Публічне управління та місцеве самоврядування*. 2024. № 2. С. 45–58. DOI: https://doi.org/10.32782/2414-4436/2024-2-9

8. Орлова Н. Євроінтеграційні орієнтири цифрової трансформації у державному управлінні України. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2025. Вип. 11. С. 118–125. DOI: https://doi.org/10.31470/2786-6246-2025-11-118-125 (дата звернення 12.09.2025).

9. Чечель А., Ангелін М. Стратегічні цифрові технології у публічному секторі України. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2024. Вип. 9. С. 176–185. DOI: https://doi.org/10.31470/2786-6246-2024-9-176-185 (дата звернення 12.09.2025).

10. Кухрівський Д. Цифрова трансформація публічного управління: тенденції та виклики. *Сучасні проблеми управління.* 2021. С. 80–89. URL: https://supproc.fsp.kpi.ua/article/view/249135 (дата звернення 12.09.2025).

11. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 р. про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у всьому Союзі (NIS Directive). URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32016L1148 (дата звернення 12.09.2025).

12. Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 р. про заходи для забезпечення високого рівня кібербезпеки в усьому Союзі (NIS2 Directive). URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX:32022L2555 (дата звернення 12.09.2025).

13. ENISA – European Union Agency for Cybersecurity. Cybersecurity Threat Landscape 2023. URL: https://enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення 12.09.2025).

14. European Commission. Risk Management in the EU Cybersecurity Frameworks. URL: https://ec.europa.eu/digital-strategy/cyber-risk-management (дата звернення 12.09.2025).

15. Digital Operational Resilience Act (DORA). URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (дата звернення 12.09.2025).

16. Європейська комісія. Європейська стратегія кібербезпеки на цифрове десятиріччя (2020–2025). URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (дата звернення 12.09.2025).

17. Самойленко Л. Цифрова трансформація публічного управління та політики: роль публічної служби у забезпеченні стійкості держави. *Публічна політика і державне управління в умовах війни.* 2023. С. 22–36. URL: https://jppasa.donnu.edu.ua/article/view/17165?utm_source=chatgpt.com (дата звернення 12.09.2025).

18. Корсун С., Магиляс Ю. Перспективні напрями досліджень цифрової трансформації публічного управління. *Аспекти публічного управління.* 2024. № 1524. С. 10–22. DOI: https://doi.org/10.15421/152437

19. Засуха М. В. Сутність цифрової трансформації публічного управління. *Проблеми сучасних трансформацій: право, публічне управління та адміністрування.* 2024. Вип. 12. С. 45–56. DOI: https://doi.org/10.54929/2786-5746-2024-12-02-04

20. Zatonatskiy D., Horiacheva K. Digitalization and cybersecurity of critical infrastructure. *Finance of Ukraine.* 2025. Issue 3. P. 77–91. DOI: https://doi.org/10.33763/finukr2025.03.077

References:

1. Novikova N. L., & Boiko L. V. (2024) Tsyfrovizatsiia ta natsionalna bezpeka: tendentsii ta vyklyky [Digitalization and national security: Trends and challenges]. *Natsionalna bezpeka: pravo ta ekonomika – National Security: Law and Economics,* vol. (1), pp. 15–28. DOI: https://doi.org/10.51369/3083-5917-2024-1-8 (accessed September 12, 2025).

2. Pigarev Yu., Kostenyuk N. (2023) Didzhytalizatsiia publichnoho upravlinnia yak chynnyk tsyfrovoi transformatsii Ukrainy [Digitalization of public administration as a factor of Ukraine's digital transformation]. *Aktualni problemy derzhavnoho upravlinnia – Current Issues of Public Administration,* pp. 23–34.

3. Saprykin V. (2024) Otsyfrovuvannia, tsyfrovizatsiia ta tsyfrova transformatsiia publichnoho upravlinnia v Ukraini [Digitization, digitalization and digital transformation of public administration in Ukraine]. V*isnyk KNU imeni T. Shevchenka. Seriia: Derzhavne upravlinnia – Bulletin of Taras Shevchenko National University. Public Administration Series,* vol. 19(1), pp. 116–121. DOI: https://doi.org/10.17721/2616-9193.2024/19-19/22

4. Hardy M. C. (2022) Digital transformation of security institutions: Between technology and democratic values. *Journal of Public Security Innovation,* vol. 15(2), pp. 45–59.

5. Gerstein D. J. (2021) Building digital resilience: New challenges to national security. *Cybersecurity & Policy Review,* vol. 9(1), pp. 21–38.

6. Hubert A. (2023) European cybersecurity policy: Implementation of the NIS2 Directive. E*uropean Security Studies,* vol. 18(3), pp. 64–77.

7. Rudenko Ye., Shapran O., & Makhno Ye. (2024) Tsyfrova transformatsiia yak faktor pokrashchennia natsionalnoi bezpeky Ukrainy [Digital transformation as a factor of strengthening Ukraine's national security]. *Publichne upravlinnia ta mistseve samovriaduvannia – Public Administration and Local Self-Government,* vol. (2), pp. 45–58. DOI: https://doi.org/10.32782/2414-4436/2024-2-9

8. Orlova N. (2025) Yevrointehratsiini oriientyry tsyfrovoi transformatsii u derzhavnomu upravlinni Ukrainy [European integration vectors of digital transformation in

Ukrainian public administration] *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia – Public Administration: Concepts, Paradigm, Development, Improvement,* vol. (11), pp. 118–125.DOI: https://doi.org/10.31470/2786-6246-2025-11-118-125 (accessed September 12, 2025).

9. Chechel A. & Anhelin M. (2024) Stratehichni tsyfrovi tekhnolohii u publichnomu sektori Ukrainy [Strategic digital technologies in Ukraine's public sector]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia – Public Administration: Concepts, Paradigm, Development, Improvement,* vol. (9), pp. 176–185. DOI: https://doi.org/10.31470/2786-6246-2024-9-176-185 (accessed September 12, 2025).

10. Kukhrivskyi D. (2021) Tsyfrova transformatsiia publichnoho upravlinnia: tendentsii ta vyklyky [Digital transformation of public administration: Trends and challenges]. *Suchasni problemy upravlinnia – Modern Problems of Management,* pp. 80–89. Available at: https://supproc.fsp.kpi.ua/article/view/249135 (accessed September 12, 2025).

11. European Parliament and Council (2016) Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Available at: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32016L1148 (accessed September 12, 2025).

12. European Parliament and Council. (2022) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Available at: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX:32022L2555 (accessed September 12, 2025).

13. ENISA – European Union Agency for Cybersecurity (2023) Cybersecurity Threat Landscape 2023. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed September 12, 2025).

14. European Commission. (n.d.). Risk Management in the EU Cybersecurity Frameworks. Available at: https://ec.europa.eu/digital-strategy/cyber-risk-management (accessed September 12, 2025).

15. Digital Operational Resilience Act (DORA). URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (accessed September 12, 2025).

16. European Commission. (n.d.) The EU's cybersecurity strategy for the digital decade (2020–2025). Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (accessed September 12, 2025).

17. Samoilenko L. (2023) Tsyfrova transformatsiia publichnoho upravlinnia ta polityky: rol publichnoi sluzhby u zabezpechenni stiikosti derzhavy [Digital transformation of public governance and policy: The role of civil service in ensuring state resilience]. *Publichna polityka i derzhavne upravlinnia v umovakh viiny – Public Policy and Governance in the Conditions of War,* pp. 22–36. Available at: https://jppasa.donnu.edu.ua/article/view/17165 (accessed September 12, 2025).

18. Korsun S., & Mahylias Yu. (2024) Perspektyvni napriamy doslidzhen tsyfrovoi transformatsii publichnoho upravlinnia [Promising research directions for digital transformation of public administration]. *Aspekty publichnoho upravlinnia – Aspects of Public Administration,* vol. (1524), pp. 10–22. DOI: https://doi.org/10.15421/152437

19. Zasukha M. V. (2024) Sutnist tsyfrovoi transformatsii publichnoho upravlinnia [The essence of digital transformation in public administration]. *Problemy suchasnykh transformatsii: pravo, publichne upravlinnia ta administruvannia – Problems of Modern Transformations: Law, Public Administration and Management,* vol. (12), pp. 45–56. DOI: https://doi.org/10.54929/2786-5746-2024-12-02-04

20. Zatonatskiy D. & Horiacheva K. (2025) Digitalization and cybersecurity of critical infrastructure. *Finance of Ukraine,* vol. (3), pp. 77–91. DOI: https://doi.org/10.33763/finukr2025.03.077

Стаття надійшла: 26.08.2025
Стаття прийнята: 19.09.2025
Стаття опублікована: 31.10.2025