**УДК 351.861**
**DOI https://doi.org/10.32782/1813-3401.2024.4.12**

***В. М. Кравченко***
аспірант кафедри публічного управління та землеустрою
Класичного приватного університету

# ЦИФРОВІЗАЦІЯ СИСТЕМИ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ У СФЕРІ ПРИКОРДОННОЇ БЕЗПЕКИ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

*Стаття присвячена аналізу особливостей, перспектив і ризиків впровадження цифровізації в систему публічного адміністрування у сфері прикордонної безпеки України, яка набуває особливого значення в умовах сучасних викликів, таких як транскордонна злочинність, міграційні кризи та гібридні загрози. У дослідженні детально розглянуто інноваційні технології, серед яких системи цифрового моніторингу, автоматизовані засоби аналізу ризиків, технології розпізнавання об'єктів і використання штучного інтелекту, спрямовані на підвищення ефективності управління прикордонними процесами. Окреслено переваги інтеграції цифрових платформ, включаючи підвищення оперативності управління, точності даних, забезпечення прозорості процедур і зниження корупційних ризиків завдяки автоматизації процесів. Зазначено, що цифровізація значною мірою сприяє посиленню безпеки на кордонах, створюючи передумови для швидкого та ефективного реагування на потенційні загрози. Разом з тим, виявлено ключові ризики та виклики, пов'язані із впровадженням цифрових інструментів, зокрема, питання інформаційної безпеки, недостатнього фінансування та технічного забезпечення, а також низького рівня цифрової грамотності персоналу, що гальмує інтеграцію нових технологій. Особливу увагу приділено впливу цифровізації на міжнародне співробітництво у сфері прикордонної безпеки. Підкреслено важливість обміну даними між країнами, стандартизації цифрових платформ і спільного впровадження інноваційних технологій як основи для боротьби з транскордонною злочинністю. Зазначено, що успішна цифровізація неможлива без удосконалення нормативно-правової бази, адаптації організаційної культури прикордонних відомств до нових умов, а також системного навчання персоналу з використання сучасних технологій і методів. Результати дослідження доводять, що цифровізація потребує значної консолідації ресурсів, включаючи фінансові, технічні та кадрові. Автори наголошують на необхідності належного фінансування проєктів, інвестицій у розвиток цифрової інфраструктури та кібербезпеки. Важливим аспектом є підтримка системного навчання кадрів для забезпечення ефективного впровадження технологій. Таким чином, розробка комплексної державної програми цифровізації у сфері прикордонної безпеки України, яка включатиме модернізацію технологічної інфраструктури, створення навчальних програм для персоналу та розширення міжнародного співробітництва, є важливим етапом для забезпечення національної безпеки. Актуальність дослідження підкріплюється сучасними викликами і підтверджує необхідність інтеграції найкращих практик європейських країн для досягнення високих стандартів у сфері прикордонного адміністрування.*

***Ключові слова:*** *цифровізація, публічне адміністрування, прикордонна безпека, публічне адміністрування, інноваційні технології, інформаційна безпека, кібербезпека.*

**Постановка проблеми у загальному вигляді.** Сучасні виклики, з якими стикається Україна у сфері прикордонної безпеки, вимагають впровадження інноваційних рішень для забезпечення ефективності публічного адміністрування. Застосування цифрових технологій, таких як автоматизовані системи моніторингу, розпізнавання ризиків та обміну даними, здатне підвищити прозорість, оперативність та безпеку управлінських рішень у цій галузі. Однак цифровізація, також, створює ризики, які стосуються фінансових, технічних та організаційних аспектів.

**Аналіз останніх досліджень і публікацій.** Дослідження цифровізації прикордонної безпеки активізувалися у зв'язку з гібридними загрозами, зокрема інформаційними атаками. У звітах Frontex [1] зазначено, що автоматиза-

ція прикордонних процесів сприяє зменшенню корупційних ризиків та пришвидшенню перевірок. Значний внесок у вивчення цієї тематики зробили українські дослідники. Так, С. В. Нікіфоренко досліджував інформаційне забезпечення прикордонного контролю [2], наголошуючи на важливості захисту даних в умовах сучасних викликів. Т. С. Подорожна акцентувала увагу на питаннях забезпечення інформаційної безпеки України [3] в контексті цифрових загроз, зокрема з боку РФ, підкреслюючи значення стійкості функціонування інститутів публічної влади. М. М. Синишин аналізував напрями реформування прикордонних органів [4], спрямовані на захист національних інтересів та інтеграцію сучасних технологій для посилення безпеки.

Українські дослідницькі центри, зокрема Національний інститут стратегічних досліджень, акцентують увагу на необхідності інтеграції інноваційних технологій в існуючу систему управління для посилення ефективності міжвідомчої взаємодії [5]. Висновки цих досліджень вказують на те, що цифровізація є ключовим елементом забезпечення прикордонної безпеки в сучасних умовах.

**Метою статті є – д**ослідження ролі цифровізації у сфері прикордонної безпеки; визначення ключових ризиків та переваг впровадження цифрових інструментів.

**Виклад основного матеріалу дослідження.** Цифровізація є одним із ключових трендів у модернізації системи публічного адміністрування, зокрема у сфері прикордонної безпеки. Інтеграція цифрових технологій дозволяє суттєво підвищити ефективність управління, оперативність реагування на загрози та забезпечити прозорість процедур. Завдяки сучасним рішенням, таким як автоматизація процесів, використання штучного інтелекту та розробка інноваційних платформ, прикордонні служби отримують можливість не лише покращити якість виконання своїх функцій, але й зменшити ризики, пов'язані з людським фактором. До переваг інтеграції цифрових технологій у прикордонне адміністрування можна віднести наступне:

1. Оперативність обробки даних: автоматизовані системи скорочують час на перевірку документів та ідентифікацію загроз.

2. Прозорість процесів: цифрові системи мінімізують ризики корупції за рахунок автоматизації процедур.

3. Ефективність моніторингу: використання дронів, сенсорних мереж та систем розпізнавання обличчя забезпечує безперервний контроль прикордонної зони.

На сьогодні процес цифровізації має цілий ряд викликів, які заважають його реалізації, зокрема:

1. Кібербезпека: автоматизація підвищує ризик кібератак та витоку конфіденційних даних. Наприклад, у 2022 році було зафіксовано кібератаки на системи eGate у декількох країнах ЄС, зокрема в Іспанії та Німеччині. За даними звітів Агентства Європейського Союзу з питань кібербезпеки (ENISA), під час атак використовувалися методи DDoS та спроби злому для доступу до персональних даних пасажирів. Такі атаки мали на меті дестабілізацію роботи автоматизованих пунктів пропуску, що призвело до затримок на кордонах та збільшення часу на перевірку документів. Ці інциденти підкреслюють важливість підвищення рівня захисту інформаційних систем на кордонах та необхідність регулярного оновлення засобів безпеки для протидії новітнім загрозам. Детальніше про ці випадки можна ознайомитися у звітах ENISA [6].

2. Фінансові обмеження: впровадження сучасних технологій вимагає значних інвестицій. Наприклад, у рамках програми "Цифрова Європа" (Digital Europe Programme) на цифровізацію прикордонної безпеки було виділено значні кошти. Загальний бюджет програми на 2021-2027 роки становить 7,5 мільярда євро, з яких значна частина спрямована на розвиток цифрової інфраструктури, включаючи проекти, спрямовані на підвищення безпеки та ефективності управління кордонами. Крім того, в рамках програми "Connecting Europe Facility" (CEF Digital) було виділено додаткові кошти на розвиток цифрових послуг та інфраструктури, що сприяють безпеці кордонів. У жовтні 2024 року було оголошено про відкриття нових конкурсів на загальну суму 323 мільйони євро для співфінансування розгортання цифрових інфраструктур, включаючи проекти з кібербезпеки та управління кордонами [7]. Ці інвестиції підкреслюють прагнення ЄС до посилення прикордонної безпеки шляхом впровадження сучасних цифрових технологій та інфраструктури.

3. Людський фактор: низький рівень цифрової грамотності серед персоналу прикордонних відомств може уповільнити інтеграцію технологій.

Досвід Європейського Союзу свідчить про ефективність цифровізації у прикордонній безпеці. Наприклад, у країнах Шенгенської зони застосовуються біометричні системи контролю,

які значно пришвидшують перевірку пасажирів. Однак такі системи потребують гармонізації правових норм і стандартів.

На основі аналізу впровадження автоматизованих систем прикордонного контролю та оцінок отриманих з сайту Європейської комісії [8] та Агентства ЄС з питань управління оперативним співробітництвом на зовнішніх кордонах [9] можемо побудувати наступний оціночний графік, так як точні дані про кількість автоматизованих пунктів пропуску в країнах ЄС за період з 1995 по 2023 роки є обмеженими, рис. 1.


Рис. 1. Зростання частки автоматизованих пунктів пропуску в країнах ЄС за 2023 рік

*Джерело: складено автором за даними [8–9]*

Зростання кількості автоматизованих пунктів пропуску у Шенгенській зоні, відображене на графіку, частково обумовлене підготовкою до впровадження Системи в'їзду/виїзду (Entry/Exit System, EES).

Система EES – це автоматизована система реєстрації даних про в'їзд, виїзд та відмову у в'їзді громадян третіх країн, які перетинають зовнішні кордони країн Шенгенської зони.

Доцільно більш детально дослідити Систему в'їзду/виїзду (Entry/Exit System, EES), яка спрямована на заміну штампування паспортів на сучасну електронну систему збору та обробки інформації. Ця система покликана оптимізувати прикордонний контроль, роблячи його швидшим та ефективнішим, зменшуючи адміністративне навантаження на прикордонні служби.

EES реалізується із використанням інноваційних технологій, зокрема біометричних даних, таких як розпізнавання облич та відбитків пальців, що забезпечують точну ідентифікацію мандрівників. Використання таких рішень сприяє більш надійному контролю та мінімізує можливості для шахрайства або зловживань.

Серед переваг впровадження цієї системи варто виділити кілька ключових аспектів. По-перше, система дозволяє автоматично виявляти осіб, які перебувають у зоні дії Шенгенської угоди довше дозволеного терміну, що значно посилює безпеку. По-друге, вона істотно скорочує час перевірки документів на кордоні, підвищуючи комфорт для мандрівників і зменшуючи черги. По-третє, автоматизація процесів мінімізує ризик людських помилок під час перевірки, що підвищує загальну ефективність прикордонного контролю.

Система EES планується до повного впровадження у 2024 році. Проте підготовчі роботи, зокрема встановлення необхідного обладнання та модернізація прикордонних пунктів, почалися значно раніше. Це пояснює стрімке зростання кількості автоматизованих пунктів у 2000-х та 2010-х роках, відображене на графіку.

EES є одним із ключових елементів загальної стратегії цифровізації прикордонного контролю в ЄС, що значно підвищує безпеку та зручність для мандрівників.

У сфері цифровізації прикордонної безпеки існує низка серйозних загроз, які потребують особливої уваги (рис. 2). Однією з ключових є кібератаки, які можуть паралізувати роботу прикордонних систем через вірусні або DDoS-атаки, використання шпигунського програмного забезпечення для збору конфіденційної інформації або злом автоматизованих пунктів пропуску. Значний ризик становить витік даних, спричинений як зовнішніми хакерськими атаками, так і внутрішніми помилками персоналу, наприклад, через недбале поводження з конфіденційною інформацією або фізичними носіями. Проблеми також пов’язані з низькою цифровою грамотністю персоналу: недостатнє розуміння принципів роботи новітніх систем або нехтування кібербезпекою можуть стати причиною критичних збоїв. Технічні несправності, які виникають через зношеність обладнання або його несумісність між різними країнами, доповнюють перелік ризиків, ускладнюючи повноцінну інтеграцію систем. Фінансові обмеження, зокрема недофінансування інфраструктурних проектів, закупівлі сучасного обладнання та підготовки кадрів, є ще одним бар’єром для успішної цифровізації. Нарешті, затримки у впровадженні технологій, викликані бюрократичними перепонами, відсутністю координації між країнами та тривалим ухваленням необхідного законодавства, суттєво сповільнюють прогрес у цій сфері. Усі ці фактори потребують комплексного підходу для забезпечення ефективності цифрових рішень у сфері прикордонної безпеки [10].

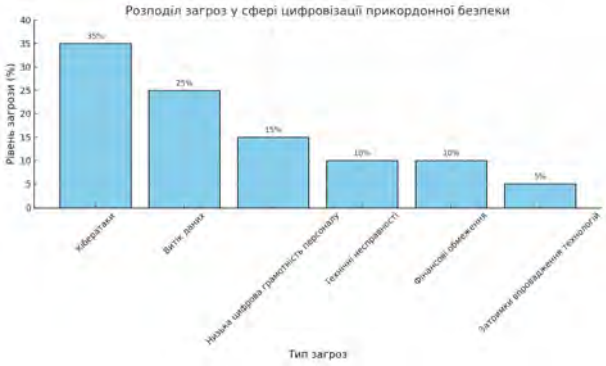


Рис. 2. Розподіл загроз у сфері цифровізації прикордонної безпеки (кіберзагрози, фінансові ризики)

*Джерело: складено автором за даними [10]*

Плани європейських муніципалітетів щодо майбутніх інвестицій у цифрову інфраструктуру демонструють значні регіональні відмінності, але загалом інвестиції або збільшуються, або залишаються на тому ж рівні (рис. 3). Згідно з даними, наведеними в звіті "Digitalisation in Europe 2022–2023"[11], близько 30% муніципалітетів у Центральній та Східній Європі планують збільшити інвестиції в цифрову інфраструктуру в період 2022–2026 років, тоді як у Південній Європі цей показник становить 40%. Більшість муніципалітетів у всіх регіонах планують зберегти інвестиції на тому ж рівні: у Північній та Західній Європі таких 50%, що свідчить про відносну стабільність їх підходу до цифрової трансформації. Лише невеликий відсоток муніципалітетів планують зменшити інвестиції – 25% у Північній та Західній Європі, що може свідчити про певні фінансові чи інші обмеження. Загалом ці тенденції вказують на стабільний або зростаючий рівень інвестицій у цифрову інфраструктуру, що є позитивним сигналом для майбутньої цифрової трансформації європейських муніципалітетів.

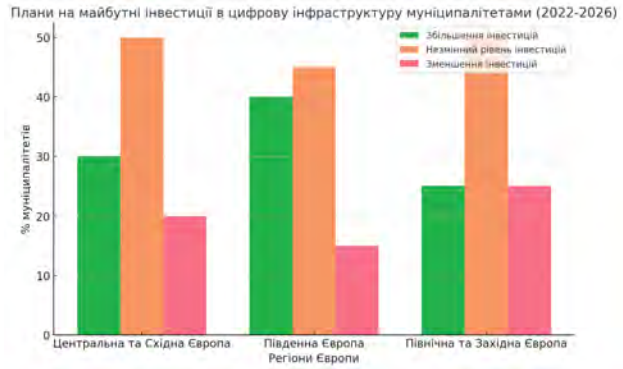


Рис. 3. Плани на майбутні інвестиції в цифрову інфраструктуру

*Джерело: складено автором за даними [11]*

Отже, на сьогодні, для України особливо актуальним стає питання розробки комплексної державної програми цифровізації прикордонної безпеки, що допоможе посилити захист кордонів в умовах сучасних викликів. Така програма має включати не лише технічну модернізацію, але й створення навчальних програм для підвищення цифрової грамотності персоналу, що працює на кордонах. Важливим аспектом є підвищення рівня компетенцій та навичок працівників у використанні сучасних технологій, що забезпечить ефективну роботу в умовах цифрових загроз. Крім того, розширення міжнародного співробітництва у сфері обміну даними може стати ключовим елементом для забезпечення безпеки та надійності кордонів. Співпраця з іншими країнами дозволить інтегрувати передові рішення та обмінюватися критично важливою інформацією, що підвищить рівень безпеки на кордонах України.

**Висновки.** У сучасних умовах цифровізація прикордонної безпеки стає невід'ємною частиною ефективного публічного адміністрування. Впровадження цифрових технологій, таких як автоматизовані системи моніторингу, розпізнавання ризиків та обміну даними, дозволяє забезпечити оперативність, прозорість та підвищену безпеку прикордонних процесів. Однак для досягнення максимального ефекту необхідно вирішувати існуючі виклики, зокрема забезпечення кібербезпеки, підвищення цифрової грамотності персоналу та подолання фінансових обмежень. Розробка комплексної державної програми цифровізації прикордонної безпеки в Україні, створення навчальних програм та розширення міжнародного співробітництва можуть стати вирішальними кроками на шляху до підвищення ефективності прикордонної безпеки та захисту національних інтересів. Загалом, інвестиції в цифрову інфраструктуру демонструють тенденцію до стабільного або зростаючого рівня, що є позитивним сигналом для майбутньої цифрової трансформації. Україні варто скористатися досвідом європейських країн для інтеграції передових технологій та досягнення високих стандартів прикордонного адміністрування.

**Список використаної літератури:**

1. Risk Analysis for 2023–2024: Frontex Report. URL: https://www.frontex.europa.eu/publications/risk-analysis-for-2023-2024-IqbX2a.
2. Нікіфоренко С.В. Інформаційне забезпечення прикордонного контролю у пунктах пропуску

через державний кордон України для повітряного сполучення. Національна академія Державної прикордонної служби України імені Богдана Хмельницького, 2021. URL: https://dspace.nadpsu.edu.ua/bitstream/123456789/2826/1/Кушн_р____нформац_йне_забезпечення_прикордонного_контролю.pdf.
3. Подорожна Т.С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. Електронний репозитарій ДВНЗ "УжНУ", 2023. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/66483.
4. Синишин М.М. Напрямки забезпечення прикордонної безпеки. Вісник національного університету цивільного захисту України, 2022. URL: https://vdu-nuczu.net/ua/11-ukr/storinkaavtora/253-sinishin-m-m-napryami-zabezpechennya-prikordonnoji-bezpeki-ukrajini (Дата звернення: 15.11.2024).
5. Інноваційні перетворення на транспорті як чинник модернізації транспортно-дорожнього комплексу України: аналітична записка. Національний інститут стратегічних досліджень. URL: https://www.niss.gov.ua/doslidzhennya/ekonomika/innovaciyni-peretvorennya-na-transporti-yak-chinnik-modernizacii.
6. Звіт ENISA Threat Landscape 2022: European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
7. Відкриття тендерів на суму 323 мільйони євро для підтримки сучасної цифрової інфраструктури під програмою «З'єднуючи Європу»: Пресреліз Європейської Комісії. URL: https://digital-strategy.ec.europa.eu/en/news/commission-opens-calls-worth-eu323-million-support-advanced-digital-connectivity-infrastructures.
8. Офіційний вебсайт Європейської Комісії. URL: https://ec.europa.eu/ (Дата звернення: 15.11.2024).
9. Офіційний вебсайт Агентства Європейського Союзу з питань охорони зовнішніх кордонів (Frontex). URL: https://frontex.europa.eu/.
10. Галіпчак В.Д. Сучасні виклики та стратегії забезпечення інформаційної безпеки україни в умовах російської агресії: перспективи та завдання. Журнал регіональні студії, 2023. URL: http://regionalstudies.uzhnu.uz.ua/archive/35/10.pdf.
11. Цифровізація в Європі 2022–2023: дані з опитування про інвестиції ЄІБ. Звіт Європейського інвестиційного банку. URL: https://www.eib.org/attachments/lucalli/20230112_digitalisation_in_europe_2022_2023_en.pdf.

**Kravchenko V. M. Digitalization of the public administration system in border security: prospects and challenges**

*The article focuses on analyzing the features, prospects, and risks of implementing digitalization in the public administration system within the sphere of Ukraine's border security, which gains particular importance in the context of modern challenges such as cross-border crime, migration crises, and hybrid threats. The study provides a detailed examination of innovative technologies, including digital monitoring systems, automated risk analysis tools, object recognition technologies, and artificial intelligence, aimed at enhancing the efficiency of border management processes. The advantages of integrating digital platforms are outlined, including improved operational efficiency, data accuracy, process transparency, and reduced corruption risks through process automation. It is noted that digitalization significantly contributes to strengthening border security, creating conditions for rapid and effective responses to potential threats. At the same time, key risks and challenges associated with the implementation of digital tools have been identified, such as information security issues, insufficient funding and technical resources, as well as low digital literacy levels among personnel, which hinder the integration of new technologies. Special attention is paid to the impact of digitalization on international cooperation in the field of border security. The importance of data exchange between countries, standardization of digital platforms, and joint implementation of innovative technologies as a foundation for combating cross-border crime is emphasized. It is stated that successful digitalization is impossible without improving the regulatory framework, adapting the organizational culture of border agencies to new conditions, and systematically training personnel in the use of modern technologies and methods. The study's results demonstrate that digitalization requires significant resource consolidation, including financial, technical, and human resources. The authors highlight the necessity of adequate funding for projects, investments in the development of digital infrastructure and cybersecurity. A critical aspect is supporting systematic staff training to ensure effective technology adoption. Thus, the development of a comprehensive national program for digitalizing border security in Ukraine, which includes technological infrastructure modernization, creation of training programs for personnel, and expansion of international cooperation, is an important step toward ensuring national security. The relevance of the study is reinforced by contemporary challenges and underscores the need to integrate best practices from European countries to achieve high standards in border administration.*

***Key words:*** *digitalization, public administration, border security, innovative technologies, information security, cybersecurity.*