DOI 10.37491/UNZ.111.7
УДК 351:004:338.246.025:351.74 (477)

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 3 (111), С. 120-129

Інна ШЕВЧУК[1], Віталій ДАНЧЄВ[2]

ЦИФРОВА ТРАНСФОРМАЦІЯ ПУБЛІЧНОЇ СЛУЖБИ ЯК ІНСТРУМЕНТ ДЕТІНІЗАЦІЇ ЕКОНОМІКИ ТА ЗАБЕЗПЕЧЕННЯ ПРИКОРДОННОЇ БЕЗПЕКИ УКРАЇНИ

Досліджено вплив цифровізації публічної служби на ефективність системи національної безпеки. Розглянуто впровадження інноваційних цифрових інструментів у діяльність прикордонних органів як стратегічний пріоритет захисту державних кордонів. Проаналізовано роль цифрових компетенцій службовців у забезпеченні стійкості державних інституцій до гібридних загроз. Визначено, що цифрова трансформація публічного управління є критичним фактором захисту національних інтересів, який забезпечує швидкість прийняття рішень, прозорість процесів та інтеграцію у міжнародний безпековий простір. Особливу увагу приділено використанню технологій штучного інтелекту, аналізу великих даних (Big Data) та біометричної ідентифікації для прогнозування безпекових ризиків. Важливо протидіяти кіберзагрозам і забезпечувати якісне безперебійне функціонування та відновлення цифрових активів внаслідок зовнішніх утручань чи руйнування, що для прикордонної безпеки України є наразі одним із стратегічних пріоритетів. Проаналізовано міжнародний досвід впровадження систем інтегрованого управління кордонами

[1] докторка наук з державного управління, професорка, завідувачка науково-дослідної частини, професорка кафедри публічного управління та адміністрування, Хмельницький університет управління та права імені Леоніда Юзькова, *innashevchuk555@gmail.com*, https://orcid.org/0000-0001-9062-8907.
[2] аспірант, Хмельницький університет управління та права імені Леоніда Юзькова, v_*danchiev@univer.km.ua*, https://orcid.org/0009-0006-3451-6744.

(ІВМ), зокрема стандарти ЄС та агентства Frontex. Європейська модель, що відповідає стандартам ЄС та настановам Frontex, є найбільш прийнятною моделлю трансформації концепції та системи національної безпеки, зокрема в частині посилення прикордонної безпеки. Визначено, що інтеграція інноваційних рішень у роботу публічних службовців підвищує оперативність реагування на гібридні загрози та забезпечує цифровий суверенітет держави в умовах глобальних викликів. Цифрова трансформація публічної служби вимагає паралельного розвитку кіберрезильєнтності. Захист державних реєстрів має розглядатися не лише як технічне завдання, а й як стратегічна умова збереження державного суверенітету в інформаційній сфері. Доведено, що в умовах гібридних загроз цифровізація публічної служби — це спосіб досягнення «цифрового суверенітету», створення екосистеми, де дані захищені, а рішення приймаються миттєво на основі точних алгоритмів.

Ключові слова: прикордонна безпека, національна безпека, інтегроване управління кордонами, публічна служба, публічне управління, цифровізація, цифрова трансформація, кіберрезильєнтність, штучний інтелект.

Постановка проблеми. В архітектурі забезпечення національної безпеки України трансформація економічних процесів та модернізація системи прикордонного контролю перебувають у стані діалектичного взаємозв'язку. Масштабна інституціоналізація тіньового сектору економіки, що реалізується через митні та прикордонні правопорушення, безпосередньо деформує фінансову систему, нівелює засади добросовісної ринкової конкуренції та позбавляє державний бюджет ресурсів, необхідних для капіталізації оборонного сектору. За цих умов цифрова трансформація публічної служби розглядається як фундаментальний архітектурний інструмент подолання корупційних зв'язків та імперативний фактор легалізації економічної діяльності. Актуальність дослідження означеної тематики зумовлена необхідністю оперативного реагування на гібридні загрози, оскільки сучасні виклики національній безпеці вимагають впровадження високотехнологічних інструментів моніторингу державного кордону та забезпечення прикордонної безпеки. Трансформація управлінських процесів стає пріоритетним завданням, тому що інтеграція інтелектуальних систем у роботу прикордонних відомств дозволяє мінімізувати корупційні ризики та помилки, зумовлені людським фактором під час прийняття стратегічних рішень. Цифрова стійкість державних інституцій є фундаментом національної стабільності, особливої ваги набуває захист інформаційного простору від кібератак, спрямованих на дестабілізацію критичної інфраструктури. Важливо зауважити, що забезпечення прикордонної безпеки в умовах глобалізації неможливе без створення єдиних баз даних, які б гарантували швидкий обмін інформацією між різними суб'єктами публічного адміністрування. Науковий інтерес до цієї проблематики посилюється через те, що

ISSN 2078-9165 Університетські наукові записки, 2026, №3 (111), С.120-129. unz.univer.km.ua

цифрові аспекти публічної служби безпосередньо впливають на ефективність виявлення протиправної діяльності, пов'язаної з нелегальною міграцією та контрабандою. Необхідно враховувати міжнародний досвід правового регулювання електронного урядування, щоб адаптувати національне законодавство до стандартів ЄС у сфері безпеки кордонів та захисту персональних даних.

Серед науковців, які займалися цією проблематикою, слід назвати таких українських учених, як: К. Ю. Бобровнікова, Є. С. Гончаров, М. О. Левицький, С. М. Лисенко, М. М. Литвин, О. І. Нікітенко, В. Нікіфоренко, О. О. Морохов, В. С. Харченко, О. Ф. Шенько, Р. В. Щука, — та іноземних — К. Бочеан, А. Варзару та Н. Гуельфі.

Мета статті — теоретичне обґрунтування та розробка практичних рекомендацій щодо вдосконалення цифрових аспектів функціонування публічної служби, які спрямовані на посилення захисту національних інтересів та підвищення ефективності системи забезпечення прикордонної безпеки в умовах сучасних глобальних викликів та гібридних загроз.

Виклад основного матеріалу. Масштабна інституціоналізація тіньових економічних процесів через призму транскордонних та митних правопорушень безпосередньо дестабілізує фінансову систему країни. Така деструкція не лише руйнує конкурентне середовище на внутрішньому ринку, а й позбавляє бюджет фіскальних надходжень. У контексті сучасних безпекових викликів це спричиняє критичний дефіцит бюджетних асигнувань, які мають спрямовуватися на фінансове забезпечення та зміцнення оборонного потенціалу України. Тінізація економічних процесів у прикордонній сфері супроводжується низкою деструктивних явищ, серед яких ключовими є:

1) умисне заниження митної вартості імпортованих субстратів, функціонування каналів «сірого» імпорту за підробленою документацією та нелегальний транзит підакцизної продукції поза межами митного контролю, що зумовлює хронічний дефіцит бюджетних надходжень (ПДВ, мита, акцизних зборів);

2) незаконне виведення капіталу в офшорні та інші юрисдикції за допомогою фіктивних фінансово-господарських операцій;

3) функціонування прихованих мереж у прикордонних регіонах, які виступають джерелом капіталізації організованої транскордонної злочинності.

Вплив глобальної цифровізації на архітектуру національної та прикордонної безпеки характеризується докорінною зміною парадигми публічного управління, де технологічний складник стає визначальним фактором збереження суверенітету. Так, розширено поняття «державний кордон», додаючи до фізичного простору віртуальний (кіберпростір). Науковці акцентують увагу, що в умовах сьогодення державний кордон є «… простором активної соціально-економічної взаємодії, потребує комплексного та скоординованого управління [1, с. 385], зауважують на необхідності «… підтримки балансу між забезпеченням належного рівня прикордонної

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 3 (111), С. 120-129

безпеки і збереженням відкритості державного кордону для законного транскордонного співробітництва, а також для осіб, які подорожують» [2, с. 9]. Є. С. Гончаров та О. І. Нікітенко об'єктом безпеки в прикордонній сфері визначають суверенітет, територіальну цілісність держави, конституційні права та свободи громадян тощо [3, с. 26].

Архітектура національної безпеки переорієнтовується на створення такої системи захисту, де цифрові бар'єри стають такими ж важливими, як і фізичні загородження, що, у свою чергу, вимагає від суб'єктів публічної служби впровадження інтелектуальних систем раннього виявлення загроз, які здатні ідентифікувати аномальну активність у режимі реального часу. У сфері прикордонної безпеки активно впроваджується концепція «розумний кордон» [4], що передбачає застосування БпЛА та супутникових технологій для дистанційного моніторингу та зондування за важкодоступними ділянками; багаторівневу біометричну ідентифікацію для підвищення якості та швидкості пропускної здатності митниць, пунктів пропуску із забезпеченням належного рівня контролю (відбитки пальців, геометрія обличчя, аналіз ходи та голосу); використання датчиків та запровадження e-Gates для мінімізації впливу людського фактора, фокусування уваги на суб'єктах/об'єктах із високим профілем ризику, формування цілісної цифрової карти державного кордону (зниження ймовірності помилки в експертизі документів).

Штучний інтелект дає змогу моделювати можливі сценарії порушення цілісності державних кордонів та виявляти приховану транскордонну злочинність, прогнозувати черги на пунктах пропуску з метою попередження заторів та підвищення ефективності охорони кордону, що трансформує архітектуру безпеки з реактивної в проактивну. ШІ-моделі інтегруються у системи відеоспостереження та БпЛА для автоматичного виявлення об'єктів у прикордонній смузі, розпізнавання номерних знаків та навіть психоемоційного стану осіб під час проходження контролю. Таким чином, відбувається прогнозований перехід від паперових носіїв (паперові журнали, архівні справи тощо) до електронних реєстрів, що забезпечує прозорість проходження кордону, зменшення часу на перевірку даних та нівелює бюрократію, посилює міжвідомчу взаємодію та створення спільного інформаційного простору для швидкої ідентифікації особи, особливо у випадках перебування особою в розшуку чи за наявності обмежень на виїзд з країни.

Алгоритмізація процесів сприяє аналізу поведінкових патернів та логістичних маршрутів, автоматично виокремлюючи аномалії, що можуть свідчити про підготовку до контрабанди або нелегальної міграції. У таких реалія безсумнівно змінюється і роль публічного службовця — перехід від ролі реєстратора до аналітика із посиленим захистом «цифрового кабінету» через складний протокол аутентифікації, застосування технології блокчейну та штучного інтелекту в умовах функціонування системи ризик-менеджменту.

В. С. Нікіфоренко та О. О. Морохов справедливо наголошують на необхідності зміцнення кадрового потенціалу органів та підрозділів охорони

ISSN 2078-9165 Університетські наукові записки, 2026, №3 (111), С.120-129. unz.univer.km.ua

державного кордону, зокрема питання мотивації та соціального супроводу [9], особливо в умовах трансформації державної політики у сфері забезпечення прикордонної безпеки та об'єктивної потреби зміни системи освіти із урахуванням стандартів НАТО [5]. Цифрова гігієна та захищеність відомчих мереж прикордонних служб є критичними для запобігання витоку конфіденційної інформації про переміщення військ, вантажів чи стратегічних ресурсів. Важливо чітко дотримуватися плану реагування на кіберінциденти, зокрема щодо визначення команди реагування та розподілу ролей; періодичного моніторингу реєстрів та баз даних, систематичне проведення тренінгів для працівників; підготовка протоколу дій за появи лагів чи інциденту ліквідації наслідків; застосування інструментів відновлення системи та коригування політики безпеки відповідного суб'єкта.

Окремо варто наголосити на резильєнтності та кіберрезильєнтності (кіберстійкості) публічної служби. Н. Гуельфі трактує «резильєнтність» як розвиток концепції гарантоздатності в контексті впливу змін на надійність системи [6]. Низка науковців дотримуються позиції, що «… гарантоздатність є інтегрованою концепцією, яка включає такі ключові атрибути, як: готовність (*availability*) — можливість системи надавати послугу в будь-який момент; безвідмовність (*reliability*) — здатність системи надавати послугу протягом визначеного проміжку часу; функційна безпека (*safety*) — можливість системи до надання послуг у заданих умовах без катастрофічних наслідків для користувачів і зовнішнього середовища; цілісність (*integrity*) — відсутність неналежної зміни системи; обслуговуваність (*maintainability*) — здатність системи бути відновленою до стану, в якому вона може правильно надавати послуги; конфіденційність (*confidentiality*) — відсутність несанкціонованого розголошення інформації» [7, с. 19]. К. Бочеан та А. Варзару розглядали взаємозв'язок між цифровою трансформацією, сталим розвитком та економічними показниками, відповідно сталий розвиток під впливом цифрової трансформації визначали як цифрову стійкість [8].

Важливо протидіяти кіберзагрозам й забезпечувати якісне безперебійне функціонування та відновлення цифрових активів внаслідок зовнішніх утручань чи руйнування, що для прикордонної безпеки України є наразі одним із стратегічних пріоритетів. Тобто мова йде не просто про захист інформаційної системи та охорону державного кордону, а про адаптивність системи на засадах невідворотності деструктивного впливу та забезпечення роботи в обмеженому або автономному режимі реєстрів та системи митного контролю при спробах несанкціонованого проникнення чи DDoS-атак. Варто відзначити, що в період 2024–2026 років кількість кібератак на державні ресурси України суттєво зросла: загальна кількість інцидентів збільшилась на 37 %; атаки на сектор безпеки та оборони — на 3,9 %; атаки на урядові організації — на 32 %; фішингові атаки — на 105 % [9; 10]. Посилюється тенденція до кіберфізичної синхронізації, коли хакери координують локацію ударів ракет, хоча постійно розробляються нові стандарти захисту інформаційної системи. Попри це, потрібно постійно моніторити стан реєстрів і баз даних, які є привабливими для хакерів. Так, у 2024 році

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 3 (111), С. 120-129

відбулася найпотужніша атака на державні реєстри України, що посилило важливість питань захисту та кібергігієни [11–14].

Важливо зосереджувати увагу на роботі систем виявлення та протидії втручанням через моніторинг мережевого трафіку, постійного аналізу даних та на постійній гігієні кіберпростору, уникаючи використання уразливих каналів зв'язку, неперевірених пристроїв, розмежування прав доступу до даних на основі окремого акаунту, внесення всіх облікових записів та доступу до інформації, безпосередньо дотичної до посадових обов'язків. Кіберстійкість актуалізує необхідність відповідної нормативної та інституційної бази, чітких протоколів взаємодії між суб'єктами на засадах аудиту, тестування та своєчасного реагування на інциденти в досліджуваній сфері.

Нові виклики та загрози сфері національної безпеки України засвідчили потребу в удосконаленні механізмів захисту та охорони кордону, тому важливо посилити міжнародне співробітництво у прикордонній сфері, сутність якого полягає в поєднанні політичних, правових і практичних інструментів, націлених на протидію транскордонним загрозам, зміцнення режиму державного кордону та сприяння законному переміщенню осіб і товарів. Суттєвими компонентами цього процесу є інтегроване управління кордонами, обмін даними, організація спільних операцій та урегулювання прикордонних інцидентів. Європейська модель, що відповідає стандартам ЄС та настановам Європейського агентства з прикордонної та берегової охорони (*Frontex*), є найбільш прийнятною моделлю трансформації концепції та системи національної безпеки, зокрема в частині посилення прикордонної безпеки. Юридичне закріплення оновленого статусу співробітництва з *Frontex* (на основі Угоди про статус) дозволяє залучати постійний корпус Агентства до операцій на території України, що, у свою чергу, потребує чіткої регламентації повноважень іноземних офіцерів та чітких протоколів спільного застосування технічних засобів. Frontex сприяє у впровадженні моделі аналізу ризиків та забезпечує технічну операційну сумісність у частині стандартизації підходів до сенсорних систем, біометричних сканерів БпЛА для ефективної взаємодії прикордонних відомств різних країн у межах спільних операцій у трьох напрямах — внутрішньовідомчому, міжвідомчому та міжнародному. Відповідно актуалізується нагальна потреба трансформації парадигми національної безпеки України, оскільки в умовах глобальної цифровізації архітектура національної безпеки еволюціонує від традиційної охорони фізичних кордонів до створення багаторівневого інтелектуального цифрового контуру, тому цифрові аспекти публічної служби стають визначальним чинником забезпечення стійкості держави перед гібридними загрозами. Важливо створювати умови для функціонування інтелектуальних мереж, оскільки впровадження технологій штучного інтелекту та біометричної ідентифікації дозволяє перейти до предикативної моделі управління кордонами, що мінімізує вплив суб'єктивного чинника («людського фактору») та підвищує точність ідентифікації безпекових ризиків без зниження пропускної здатності пунктів пропуску. Водночас цифрова трансформація публічної служби вимагає паралельного

ISSN 2078-9165 Університетські наукові записки, 2026, №3 (111), С.120-129. unz.univer.km.ua

розвитку кіберрезильєнтності. Захист державних реєстрів має розглядатися не лише як технічне завдання, а й як стратегічна умова збереження державного суверенітету в інформаційній сфері.

Реконцептуалізація публічної служби на засадах цифровізації трансформує філософію державного контролю з каральної на проактивно-аналітичну. Відповідно системна детінізація досягається шляхом застосування таких цифрових інструментів:

— впровадження безконтактних цифрових інтерфейсів (зокрема автоматизованого митного клірингу, електронних систем верифікації черг та сертифікатів походження) сприятиме мінімізації безпосередньої взаємодії між суб'єктами господарювання та представниками публічної служби, що ліквідує передумови для отримання корупційної ренти;

— інтеграція та синергетичний обмін даними між інформаційними контурами Державної прикордонної служби України, Державної митної служби України та Державної податкової служби (у поєднанні з європейськими системами, такими як NCTS) дозволяє сформувати наскрізний цифровий трекінг товару, що, у свою чергу, унеможливлює використання фіктивних схем податкового кредиту та легалізацію контрабандного субстрату на внутрішньому ринку;

— застосування технологій ШІ та предиктивної аналітики Big Data для динамічного профілювання транскордонних ризиків у реальному часі.

Тобто цифровізація зазначеного сегмента формує стійкий фінансово-економічний базис для довгострокового забезпечення національної безпеки України в умовах сучасних викликів та загроз.

Для вдосконалення цифрових аспектів функціонування публічної служби, спрямованих на посилення захисту національних інтересів та підвищення ефективності системи забезпечення прикордонної безпеки в умовах сучасних глобальних викликів і гібридних загроз, важливо реалізувати кілька кроків. По-перше, розглянути можливість створення єдиної розвідувально-аналітичної платформи на базі штучного інтелекту; по-друге, розгортання автономних сенсорних мереж та БПЛА для моніторингу «зеленого» кордону; по-третє, повна ізоляція прикордонних ІТ-систем від публічного інтернету, шифрування каналів за національними стандартами та багатофакторна автентифікація для кожного посадовця; по-четверте, модернізація пунктів пропуску сканерами біометричних даних нового покоління (геометрія обличчя, райдужка ока) та системами перевірки цифрових паспортів (використання технологій Liveness Detection для виявлення силіконових масок, підроблених цифрових профілів у смартфонах та згенерованих штучним інтелектом фото/відеодокументі).

Висновки. Таким чином, подальша розбудова цифрової держави є ключовим фактором зміцнення суверенітету, забезпечення національної та прикордонної безпеки, адже технологічна перевага стає вирішальним аргументом у протистоянні зовнішнім гібридним загрозам, що, у свою чергу, вимагає від публічних службовців високого рівня цифрової грамотності та здатності працювати в умовах постійної модернізації технологіч-

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 3 (111), С. 120-129

ного забезпечення в умовах гібридних загроз цифровізації публічної служби — це спосіб досягнення «цифрового суверенітету», створення екосистеми, де дані захищені, а рішення приймаються миттєво на основі точних алгоритмів.

Важливо наголосити, що цифрова трансформація публічної служби у сфері економічної та прикордонної безпеки — це про реконцептуалізацію та реконфігурацію архітектури державного управління, в першу чергу, оскільки такий глобальний крок передбачає передбачає перехід до моделі *«держави як платформи»* (Government as a Platform), де управлінські процедури максимізують прозорість, усувають суб'єктивний людський фактор та мінімізують витрати для суб'єктів господарювання, що є першоосновою для зниження рівня системної корупції.

Цифровізація публічних послуг безпосередньо впливає на детінізацію національної економіки шляхом інтеграції державних реєстрів та фіскальних баз даних; здійснення превентивного моніторингу підозрілих фінансово-господарських операцій у режимі реального часу на основі технологій штучного інтелекту та аналізу великих даних (Big Data); переведення взаємодії між бізнесом та державою в безконтактну цифрову площину.

Впровадження новітніх цифрових технологій у діяльність публічної служби в прикордонній сфері безпосередньо посилює оборонний та безпековий потенціал держави через розгортання інтелектуальних систем інтегрованого управління кордонами; автоматизований аналіз міграційних та пасажиропотоків; безперешкодний горизонтальний обмін даними між Державною прикордонною службою, Державною митною службою, правоохоронними органами та силами оборони. Відтак успішна реалізація цифрового потенціалу публічної служби в Україні стримується низкою безпекових викликів, головними з яких є загрози кібератак на об'єкти критичної інформаційної інфраструктури та дефіцит кваліфікованих ІТ-кадрів у державному секторі.

Подальший розвиток досліджуваної сфери потребує гармонізації національного цифрового законодавства зі стандартами ЄС та НАТО, а також безперервного підвищення рівня цифрової грамотності публічних службовців.

Список використаних джерел

1. Левицький М. О., Шенько О. Ф. Міжнародне співробітництво Державної прикордонної служби України у сфері забезпечення прикордонної безпеки: правові засади, сутність та форми реалізації. *Аналітично-порівняльне правознавство*. 2025. Т. 3, № 5. С. 384–389. https://doi.org/10.24144/2788-6018.2025.05.3.57.
2. Нікіфоренко В., Нгуєн А. Міжнародне співробітництво як інструмент управління міграцією. *Migration & Law*. 2021. Vol. 1, Iss. 2. С. 5–18. https://doi.org/10.32752/2786-5185-2021-1-2-5-18.
3. Гончаров Є. С., Нікітенко О. І. Сутність та особливості забезпечення безпеки в прикордонній сфері правоохоронними органами. *Науковий вісник Ужгородського національного університету. Серія Право*. 2016. Вип. 36. Т. 2. С. 24–26. URL: https://t.ly/18FHF.

ISSN 2078-9165 Університетські наукові записки, 2026, №3 (111), С.120-129. unz.univer.km.ua

4. Сушко І. Аналітична записка «Розумні кордони» в Україні. *ISMPD*. URL: https://t.ly/r0Jdo.
5. Нікіфоренко В. С., Морохов О. О. Стратегічні пріоритети діяльності Державної прикордонної служби щодо забезпечення національної безпеки України. *Український політико-правовий дискурс*. 2025. № 11. https://doi.org/10.5281/zenodo.15488344.
6. Guelfi N. A formal framework for dependability and resilience from a software engineering perspective. *Central European Journal of Computer Science*. 2011. No. 1. P. 294-328. https://doi.org/10.2478/s13537-011-0025-x.
7. Лисенко С. М., Харченко В. С., Бобровнікова К. Ю., Щука Р. В. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія. *Радіоелектронні і комп'ютерні системи*. 2020. № 1 (93). С. 17–28. https://doi.org/10.32620/reks.2020.1.02.
8. Bocean C., Varzaru A EU countries' digital transformation, economic performance, and sustainability analysis. *Humanities and Social Sciences Communications*, 2023. № 10. Art. 875. https://doi.org/10.1057/s41599-023-02415-1.
9. Рекордна кількість кібератак: РНБО відзвітувала про 6 тисяч інцидентів у 2025 році (23.02.2026). *Всвіті*. URL: https://t.ly/MAUnd.
10. Тарчинець М. 6 тисяч кібератак проти України здійснили у 2025 році, на 37 % більше ніж у попередньому — РНБО (20.02.2026; 19:20). *AIN.UA*. URL: https://t.ly/mdG7O.
11. Кібератака на державні реєстри України (2024). *Вікіпедія*. URL: https://t.ly/Escp-
12. Кібератаки на бізнес України 2025: Нові вектори загроз та захист. *Synchron*. URL: https://t.ly/zRc_e.
13. Порощук Н. Кібербезпека України. Що покращилося за рік після прийняття євроінтеграційного закону (15.04.2026; 22:00). *Главком*. URL: https://t.ly/ylVm8.
14. Кіберстійкість державних реєстрів: ДП «НАІС» після кібератаки вийшло на новий курс (05.09.2025). *ДП «Національні інформаційні системи»*. URL : https://t.ly/V_QXN.

Inna SHEVCHUK, Vitaliy DANCHEV
(Leonid Yuzkov Khmelnytskyi University of Management and Law)

Digital Transformation of Public Service as a Tool for De-Shadowing the Economy and Ensuring Border Security in Ukraine

The article examines the impact of the digitalisation of public services on the effectiveness of the national security system. The introduction of innovative digital tools into the activities of border authorities is considered a strategic priority for protecting state borders. The role of digital competencies of employees in ensuring the resilience of state institutions to hybrid threats is analysed. It is determined that the digital transformation of public administration is a critical factor in protecting national interests, which ensures the speed of decision-making, transparency of processes and integration into the international security space. Particular attention is paid to the use of artificial intelligence technologies, big data analysis (Big Data) and biometric identification to predict security risks. It is important to counteract cyber threats and ensure high-quality, uninterrupted functioning and restoration of digital assets due to external interference or destruction, which, for the border security of Ukraine, is currently one of the strategic priorities. The international experience of implementing integrated border management

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 3 (111), С. 120-129

(IBM) systems is analysed, in particular, the standards of the EU and the Frontex agency. The European model, which complies with EU standards and Frontex guidelines, is the most acceptable model for transforming the concept and system of national security, particularly in terms of strengthening border security. It has been determined that the integration of innovative solutions into the work of public servants increases the efficiency of responding to hybrid threats and ensures the digital sovereignty of the state in the face of global challenges. The digital transformation of the public service requires the parallel development of cyber resilience. The protection of state registers should be considered not only as a technical task, but as a strategic condition for preserving state sovereignty in the information sphere. It has been proven that in the face of hybrid threats, the digitalisation of the public service is a way to achieve «digital sovereignty», the creation of an ecosystem where data is protected, and decisions are made instantly based on accurate algorithms.

***Keywords**: border security, national security, integrated border management, public service, public administration, digitalisation, digital transformation, cyber resilience, artificial intelligence.*

Надійшла до редакції	07.04.2026	Опублікована онлайн	22.05.2026
Прийнята до друку	20.05.2026	Опублікована	31.05.2026

Декларації

Внесок авторів. І. Шевчук — концепція дослідження, постановка проблеми, методологія, аналіз та інтерпретація матеріалів, формулювання висновків, редагування й доопрацювання тексту, загальне керівництво дослідженням. В. Данчєв — збір матеріалів, аналіз та інтерпретація матеріалів, участь у формулюванні висновків, редагування й доопрацювання тексту.

Фінансування. Дослідження виконано без зовнішнього фінансування у межах науково-дослідної роботи Хмельницького університету управління та права імені Леоніда Юзькова, зокрема наукової теми кафедри публічного управління та адміністрування «Шляхи удосконалення механізмів публічного управління та адміністрування в сфері національної безпеки в умовах євроінтеграції (державний реєстраційний № 0120U104417).

Конфлікт інтересів. Автори заявляють про відсутність конфлікту інтересів.

Використання штучного інтелекту. Інструменти штучного інтелекту під час підготовки статті не використовувалися.

Редакційна примітка. І. Шевчук входить до складу наукової ради журналу «Університетські наукові записки». Наукова рада журналу не бере участі в редакційному розгляді рукописів, організації рецензування та прийнятті рішень щодо публікації.

ISSN 2078-9165 Університетські наукові записки, 2026, №3 (111), С.120-129. unz.univer.km.ua