DOI 10.37491/UNZ.110.7
УДК 351.86:35.077.5:004 (477)

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98

Інна ШЕВЧУК[1], **Едуард ЩЕПАНСЬКИЙ**[2]

ЦИФРОВІЗАЦІЯ СИСТЕМИ ПУБЛІЧНОГО УПРАВЛІННЯ ПРИКОРДОННОЮ БЕЗПЕКОЮ ЯК ФАКТОР ОПТИМІЗАЦІЇ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Досліджено роль та значення цифровізації у трансформації системи публічного управління прикордонною безпекою. Автором обґрунтовано, що впровадження новітніх цифрових технологій (ШІ, Big Data, автоматизовані системи аналізу ризиків) є визначальним чинником оптимізації публічно-управлінських рішень. Авторами наголошено, що цифровізація змінює традиційний цикл прийняття управлінських рішень та включає такі взаємопов'язані етапи: автоматизований збір інформації; аналітична обробка та оцінка ризиків; формування альтернативних варіантів управлінських рішень; посилення застосування систем підтримки прийняття рішень (Decision Support Systems, DSS) і реалізація управлінського рішення та моніторинг результатів. Розглянуто перехід від традиційних моделей контролю до управління на основі даних (Data-driven decision making), що дозволяє мінімізувати корупційні ризики та людський фактор. Особливу увагу приділено інтеграції прикордонної складової у межах єдиного ци-

[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] доктор наук з державного управління, професор, кафедри публічного управління та адміністрування, Хмельницький університет управління та права імені Леоніда Юзькова, *eduard.shchepanskiy@gmail.com*, https://orcid.org/0000-0001-7404-3722.

фрового простору, що сприяє підвищенню ефективності реагування на гібридні загрози. Доведено, що цифровізація управлінського процесу на кордоні безпосередньо зміцнює національну безпеку держави через посилення економічної стійкості та територіальної цілісності. За результатами дослідження, запропоновано рекомендації щодо подальшого вдосконалення цифрових інструментів у діяльності публічних органів влади, зокрема розширити використання технологій штучного інтелекту та прогнозної аналітики для передбачення ризиків транскордонної злочинності та оптимізації процедур контролю; посилити впровадження моделей контролю, заснованих на оцінці ризиків; забезпечити кібербезпеку цифрових систем управління кордонами; удосконалити цифрові системи підзвітності та аудиту, які забезпечать повну прозорість та відстежуваність управлінських рішень та підвищать рівень довіри до публічних інституцій.

Ключові слова: публічне управління, цифровізація, управлінське рішення, прикордонна безпека, національна безпека, гібридні загрози, інтегроване управління кордонами, цифрова трансформація, аналіз ризиків.

Постановка проблеми. Посилення геополітичної нестабільності, перманентна ескалація воєнних конфліктів та трансформація гібридних загроз вимагають від держав переосмислення підходів до забезпечення національної безпеки, базовим елементом якої є надійне функціонування системи прикордонної безпеки, що, у свою чергу, зумовлює об'єктивну необхідність зміни інституціонально-функціонального базису публічного управління шляхом його масштабної цифрової трансформації. Інтеграція в управлінський контур сучасних інформаційно-комунікаційних технологій, зокрема, систем інтелектуального відеомоніторингу, засобів автоматизованого прикордонного контролю, безпілотних авіаційних комплексів, технологій штучного інтелекту та інструментів аналізу великих даних (Big Data) формує принципово нове цифрове середовище, що дозволяє акумулювати, верифікувати та обробляти критично важливу інформацію в режимі реального часу, забезпечуючи високу якість інформаційно-аналітичного супроводження управлінської діяльності. Водночас питання цифровізації публічного управління прикордонною безпекою як цілісного чинника оптимізації публічно-управлінських рішень залишаються недостатньо розробленими.

Серед науковців, які займалися цією проблематикою, слід назвати таких українських учених: О. Б. Ганьба, І. В. Криворучко, Д. А. Купрієнко, С. П. Кух, С. С. Ненько, О. В. Телюк, Г. Г. Чмерук, І. М. Шопіна.

Мета статті — обґрунтувати роль цифровізації як ключового інструменту трансформації публічного управління прикордонною безпекою з метою оптимізації процесу прийняття публічно-управлінських рішень задля протидії загрозам національній безпеці.

ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98. unz.univer.km.ua

Виклад основного матеріалу. У сучасній науковій літературі цифровізацію трактують як комплексний процес трансформації соціально-економічних та управлінських систем, що ґрунтується на впровадженні цифрових технологій, застосуванні даних та автоматизованих алгоритмів у всіх сферах життєдіяльності суспільства та держави. С. П. Кух відзначає, що досліджувана категорія «вживається для окреслення трансформацій, які є набагато ширшими, ніж просто заміна аналогового або фізичного на цифровий чи інформаційний ресурс [1, с. 53]. На відміну від простого перенесення інформації з паперової форми в електронну (оцифрування), цифровізація передбачає якісну зміну логіки функціонування управлінських інститутів, методів прийняття рішень та механізмів взаємодії між суб'єктами управління. У публічному управлінні цифровізація виступає як управлінська інновація системного характеру, що змінює не лише інструменти, а й саму філософію управлінської діяльності, і відбувається такий перехід від традиційної до гнучкої моделі управління, яка значною мірою базується на ієрархії та суб'єктивному досвіді чиновників, до гнучкої, орієнтованої на дані та технологічне забезпечення системи управління. Відповідно погоджуємося із позицією Г. Г. Чмерук, що «цифрова трансформація та інновації глибоко переплетені в цифровій організації. Або інновації приводять до трансформації, або успішна трансформація приводить до посилення інновацій» [2, с. 19]. І. В. Криворучко справедливо зауважує, що цифровізація сфери публічного управління спрямована на підвищення його ефективності в контексті формування цифрового суспільства на національному та глобальному рівнях [3]. С. С. Ненько наголошує, що «цифровізація публічного адміністрування, яка розглядається не лише як технічне оновлення органів влади, а й як комплексний правовий, організаційний та інституційний процес» [4, с. 161]. Ключовим принципом цифровізації в публічному управлінні є підхід, що базується на даних, тобто на використанні великих масивів структурованих та неструктурованих даних для обґрунтування управлінських рішень. У такій моделі зменшується вплив суб'єктивних оцінок та інтуїтивних суджень посадових осіб, а роль аналітики, статистичних моделей, прогнозування та штучного інтелекту зростає, що, у свою чергу, сприяє підвищенню точності управлінських рішень, їх обґрунтованості та ефективності, особливо у сфері національної безпеки, реагування на кризові ситуації та гібридні загрози. Важливою компонентою цифровізації є алгоритмізація управлінських процесів, що передбачає формалізацію процедур підготовки та прийняття рішень у вигляді чітко визначених алгоритмів, сценаріїв та протоколів дій. У публічному управлінні це означає розробку стандартизованих моделей реагування на типові ситуації, зокрема на виклики у сфері безпеки, надзвичайні події або адміністративні процедури. Алгоритмізація сприяє уніфікації управлінських практик, зменшуючи варіативність рішень у подібних ситуаціях та підвищуючи оперативність державних інституцій. Використання цифрових систем управління дозволяє фіксувати всі етапи прийняття та реалізації рішень у вигляді цифрових слідів (файлів журналів), що надає можливість подальшого аудиту, контролю та аналізу, що суттєво зменшує ризики корупції,

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98

зловживання службовим становищем та неформального впливу на управлінські рішення, оскільки кожна дія в системі фіксується та відстежується.

У сучасній науковій парадигмі національної безпеки прикордонна безпека розглядається як складова комплексної системи державного захисту, що забезпечує територіальну цілісність держави, контроль за переміщенням осіб та транспортних засобів через державний кордон, а також запобігання транскордонним загрозам, тобто набуває статусу окремого об'єкта управлінського впливу, що характеризується високим рівнем міжвідомчої взаємодії, технологічною складністю та необхідністю постійної адаптації до змін у безпековому середовищі. І. М. Шопіна трактує поняття «прикордонна безпека» як підсистему для безпеки державного кордону [5]. О. Б. Ганьба відзначає, що основою прикордонної безпеки є «територіальна цілісність України, недоторканність державного кордону й охорона суверенних прав у її прилеглій зоні та виключній (морській) економічній зоні» [6, с. 137]. Колектив науковців розглядає досліджуване поняття як захищеність життєвих інтересів у прикордонному просторі держави, протидію правопорушенням та загрозам національній безпеці [7, с. 6–7]. Д. А. Купрієнко підтримує позицію авторів, акцентуючи увагу на необхідності створення умов для розвитку особи, суспільства і держави [8, с. 362].

Питання прикордонної безпеки не можна розглядати ізольовано від інших складових національної безпеки, оскільки воно функціонально пов'язане з митною, міграційною, економічною та кримінальною безпекою. Саме тому в сучасних дослідженнях дедалі частіше застосовується інтеграційний підхід, який передбачає розгляд прикордонної безпеки як елемента єдиної системи державного управління процесами безпеки. З функціонального погляду, охорона кордонів спрямована, насамперед, на забезпечення недоторканності державного кордону та здійснення ефективного контролю за переміщенням осіб, транспортних засобів та вантажів, охоплює систему заходів щодо запобігання незаконному перетину кордону, протидії терористичним загрозам, транскордонній злочинності, нелегальній міграції та іншим ризикам, що можуть становити загрозу державному суверенітету. Відповідно прикордонна безпека виконує не лише захисну, а й регулятивну функцію, оскільки визначає правила та процедури перетину кордону, а також забезпечує їх дотримання через діяльність уповноважених державних органів, тобто є інструментом захисту державного суверенітету в прикордонній зоні.

У сучасних умовах забезпечення прикордонної та національної безпеки неможливе без інтегрованого управління кордонами (ІУК), що передбачає координацію діяльності всіх державних органів та міжнародних партнерів, що здійснюють захист та охорону державного кордону, а також налагодження ефективної взаємодії між ними. Тобто ІУК розглядається як інституційна та організаційна модель, що забезпечує синхронізацію прикордонних, митних, міграційних, правоохоронних та інших органів у єдиному управлінському циклі, тобто забезпечуючи міжвідомчу інтеграцію для уникнення дублювання функцій, підвищення ефективності використання ресурсів та забезпечення комплексного підходу до оцінки ризиків. Цифровізація відіграє особливу роль у впровадженні ІУК, оскільки саме

ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98. unz.univer.km.ua

цифрові технології створюють платформу для обміну даними між різними державними органами. У цьому контексті цифровий простір виступає інтеграційним «мостом» між митними та прикордонними органами, забезпечуючи оперативний доступ до інформації, автоматизований обмін даними та формування єдиної аналітичної платформи. Зокрема, використання уніфікованих інформаційних систем дає змогу проводити попередній аналіз ризиків ще до фактичного перетину кордону, що значно підвищує ефективність контролю та зменшує навантаження на прикордонну інфраструктуру. Крім того, інтегровані цифрові платформи забезпечують можливість обміну даними, що мінімізує інформаційну асиметрію між різними суб'єктами державного управління. Ефективність впровадження цифрових технологій суттєво залежить від правового статусу та потенціалу суб'єктів цифровізації на макро- (органи публічної влади, міністерства, профільні відомства тощо), мезо- (інституційні провайдери, бізнес-сектор) та мікрорівень (споживачі цифрових послуг), синергетична взаємодія, узгодженість інтересів та готовність до взаємодії яких забезпечуватимуть успіх цифрових трансформацій. Поряд із забезпеченням прикордонної безпеки важливо звертати увагу і на стан митної безпеки, оскільки об'єктом прикордонної безпеки є безпосередньо державний кордон, прикордонна смуга та забезпечення правопорядку у прикордонній службі, тоді як об'єктом митної безпеки є митна територія держави та митні кордони, які не завжди збігаються з географічними, тому питання цифровізації прикордонної безпеки безпосередньо стосуються і митної безпеки.

У сфері національної безпеки України цифровізація передбачає системну модернізацію інституцій, що спрямована на превенцію загроз, захисту суверенітету та територіальної цілісності, реалізується шляхом забезпечення кіберстійкості (базується на пріоритеті безпеки над сервісом та автономності критичної інфраструктури); інтероперабельності; оперативності та превентивності управління; адаптивності нормативно-правової бази до викликів та нових міжнародних стандартів; цифрових компетентностей публічних службовців та підвищення знань щодо кібергігієни.

Умови цифрової трансформації суттєво змінюють характер та структуру процесу прийняття рішень у сфері публічного управління — якщо в класичній (бюрократичній) моделі цей процес є послідовним, довготривалим та значною мірою залежить від людського чинника, то в цифровій моделі він набуває рис безперервного, автоматизованого та орієнтованого на дані управлінського циклу. О. В. Телюк акцентує увагу на тому, що «цифрові технології дозволяють забезпечити прозорість, швидкодію, інклюзивність та ефективність ухвалення управлінських рішень, що є критично важливим у період відбудови країни та відновлення довіри до влади» [9, с. 332]. Цифровізація змінює традиційний цикл прийняття управлінських рішень, інтегруючи в нього автоматизовані системи збору та аналізу даних, і в результаті формується нова архітектура управлінського процесу, що включає такі взаємопов'язані етапи:

— автоматизований збір інформації. Перший етап прийняття рішень у цифровому середовищі характеризується переходом від ручного збору інформації до автоматизованого багатоканального збору даних. Джерелами

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98

інформації є різноманітні цифрові та технічні системи – сенсорні пристрої, сканери, камери відеоспостереження, системи біометричного контролю, електронні реєстри митних та прикордонних органів, а також інтегровані бази даних державних органів. Особливістю цього етапу є безперервність та оперативність отримання даних, що дозволяє публічним органам отримувати актуальну інформацію про події без затримок, властивих традиційним адміністративним процедурам, що, своєю чергою, значно підвищує ефективність реагування на потенційні загрози;

— аналітична обробка та оцінка ризиків. Другий етап передбачає використання сучасних технологій обробки даних, зокрема штучного інтелекту (ШІ), машинного навчання та систем аналізу ризиків. На цьому рівні зібрана інформація структурується, класифікується та інтерпретується з метою виявлення потенційних загроз та суперечностей, тобто традиційна експертна аналітика трансформується в алгоритмічно підкріплений процес прийняття рішень, де значна частина аналітичних функцій делегується цифровим системам, що здатні виявляти приховані закономірності, прогнозувати ризики та формувати ймовірнісні моделі розвитку подій. У сфері прикордонної безпеки це може виявлятися у формуванні профілів ризику осіб, вантажів або транспортних засобів, що дозволяє підвищити точність контролю та зменшити кількість необґрунтованих перевірок;

— формування альтернативних варіантів управлінських рішень. Посилення застосування систем підтримки прийняття рішень (Decision Support Systems, DSS), що дає синергетичний ефект від поєднання навичок людини та алгоритмізації дій під час підготовки управлінського рішення із врахуванням можливих ризиків, тобто удосконалюється процес сценарного аналізу як інструменту стратегічного управління. Як приклад для розподілу категорій ризику на «червоний», «жовтий» та «зелений» коридор на митному контролі доцільно розглянути роботу митниці. Кінцеве рішення залишається за відповідальною особою, проте варіативність пропозицій та рекомендації цифрової системи значно підвищує результативність прийнятого рішення;

— реалізація управлінського рішення та моніторинг результатів. Реалізація рішення автоматично фіксується в системі, залишаючи цифровий слід з метою подальшої оцінки ефективності рішення та виявлення причин появи відхилень. Тобто традиційний контроль перетворюється на превентивний контроль, забезпечуючи реалізацію контролінгу як допоміжної підфункції на кожному етапі управлінського циклу, що, своєю чергою, підвищує рівень керованості системою публічного управління. Відповідно перехід від традиційних адміністративно-бюрократичних моделей контролю до моделей прийняття рішень на основі даних (DDDM) є ключовим елементом трансформації публічного управління в контексті інституційних змін та активного впровадження технологічних інновацій, що в результаті дає змогу сформувати прозору та ефективну систему публічного управління із мінімізацією впливу людського чинника та зменшення рівня корупції.

Особлива увага в сучасних дослідженнях у сфері публічного управління та національної безпеки приділяється процесам інтеграції прикордонного компонента в єдиний цифровий простір, що вважається ключовим

ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98. unz.univer.km.ua

фактором підвищення ефективності протидії гібридним загрозам. Інтеграція прикордонного компонента в такий простір означає подолання фрагментарності в комунікації та інформаційних потоках між прикордонними, митними, міграційними та правоохоронними органами. Створення єдиного цифрового простору забезпечує принципово новий рівень міжвідомчої інтеграції, що ґрунтується на взаємодії інформаційних систем та уніфікації стандартів обміну даними, що дозволяє створювати єдині аналітичні платформи управління ризиками, які в режимі реального часу накопичують інформацію з різних джерел і забезпечують комплексну оцінку ситуації з безпекою на кордоні.

У щорічному звіті Адміністрації державної прикордонної служби України для медіа і громадянського суспільства за 2025 рік відзначено, що в напрямку підвищення цифрової спроможності, ефективності реалізації прийнятих рішень та виконання повноважень суб'єктами забезпечення прикордонного контролю проведено модернізацію програмного забезпечення з функціями біометричного контролю «e-border control»; інтегровано сучасні мобільні рішення на базі захищеного планшета з функціями біометричного контролю; на першій лінії прикордонного котролю модернізовано робочі місця; протягом звітного періоду забезпечувався постійний моніторинг стану захищеності інформаційних ресурсів та превенція майбутнім потенційним інцидентам [10].

У сучасних геополітичних реаліях для України критичного значення набуває розробка та впровадження комплексної державної стратегії цифровізації системи прикордонної безпеки. Оптимізація охорони державного кордону в умовах актуальних безпекових викликів потребує не лише системної модернізації матеріально-технічної бази, а й посиленої роботи з кадровим потенціалом. Зокрема, пріоритетним завданням є розробка інноваційних освітніх програм, спрямованих на посилення цифрових компетентностей та формування високого рівня кібергігієни серед особового складу прикордонних відомств. Водночас архітектурним елементом забезпечення надійності кордонів виступає диверсифікація міжнародного співробітництва у сфері інформаційного обміну. Транскордонна інтеграція передових технологічних рішень та оперативний обмін критично важливими даними з іноземними партнерами дозволить суттєво підвищити стійкість системи національної безпеки України.

З метою подальшого удосконалення цифрових інструментів у діяльності органів публічної влади варто розширити використання технологій штучного інтелекту та прогнозної аналітики для передбачення ризиків транскордонної злочинності та оптимізації процедур контролю; посилити впровадження моделей контролю, заснованих на оцінці ризиків, що дозволяють диференціювати рівень перевірок залежно від ступеня загрози, що мінімізує адміністративне навантаження та прискорює законне переміщення осіб і товарів через кордон; забезпечити кібербезпеку цифрових систем управління кордонами, оскільки зростання обсягу оброблюваних даних збільшує вразливість інформаційної інфраструктури до зовнішніх кібератак та несанкціонованого доступу; удосконалити цифрові системи підзвітності та аудиту, які забезпечать повну прозорість та відстежуваність

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98

управлінських рішень, підвищать рівень довіри до публічних інституцій. Варто виділити кілька ключових проблем правового регулювання сфери цифровізації публічного управління прикордонною безпекою, зокрема:

1) термінологічна невизначеність (в українському законодавстві (зокрема в Законі України «Про Державну прикордонну службу України» та Стратегії інтегрованого управління кордонами) відсутнє уніфіковане нормативне закріплення таких дефініцій, як: «цифрова прикордонна безпека», «автоматизоване управлінське рішення в охороні кордону» та «цифровий суверенітет прикордонного простору»);

2) штучні бюрократичні бар'єри, що знижують ефективність та оперативність управлінських рішень (чинна нормативно-правова база не забезпечує належної легітимізації автоматичного (безлюдного) обміну даними між інформаційними системами Державної прикордонної служби, Державної митної служби та іншими суб'єктами сектору безпеки і оборони);

3) відсутність нормативної регламентації застосування штучного інтелекту;

4) неврегульованість правових механізмів кіберзахисту (нормативні акти не відповідають динамічним змінам впровадження хмарних технологій (Cloud Computing) та архітектури «нульової довіри» (Zero Trust) у специфічній сфері прикордонного контролю.

Вирішення вищезазначених потреб потребує системної та виваженої державної політики та прийняття відповідних управлінських рішень, а саме:

1) внести зміни до Закону України «Про Державну прикордонну службу України» шляхом доповнення його окремою статтею щодо цифровізації безпекових процесів, щоб закріпити поняття «цифрова інфраструктура прикордонної безпеки» та визначити правову силу управлінських рішень, згенерованих із застосуванням автоматизованих аналітичних платформ;

2) ініціювати ухвалення спеціального нормативно-правового акта з метою унормування наскрізної інтероперабельності (технічної, юридичної тощо) інформаційних систем державної прикордонної служби України, митної служби, міграційної служби та служби безпеки;

3) розробити та затвердити Постанову Кабінету Міністрів України «Про затвердження Порядку використання систем штучного інтелекту та предиктивної аналітики у сфері охорони державного кордону» з метою розмежування випадків, де ШІ виконує лише дорадчо-рекомендаційну функцію, де його алгоритми можуть автоматично блокувати транскордонні ризики, визначивши при цьому суб'єкта юридичної відповідальності (посадову особу, яка верифікує рішення).

Висновки. Отже, цифровізація системи публічного управління прикордонною безпекою є фундаментальним фактором для оптимізації управлінських рішень у сфері національної безпеки, оскільки перехід від традиційних методів контролю до високотехнологічних цифрових платформ забезпечує максимальну швидкість, точність та прозорість процесів, що безпосередньо впливає на захищеність державних кордонів шляхом реалізації таких кроків:

ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98. unz.univer.km.ua

— трансформація системи прийняття рішень (цифровізація змінює класичну вертикальну модель управління прикордонною безпекою на динамічну систему, що базується на даних (Data-driven decision making). Автоматизація збору інформації мінімізує вплив людського фактора та знижує корупційні ризики;

— впровадження штучного інтелекту та Big Data (використання алгоритмів штучного інтелекту для аналізу великих масивів даних (Big Data) дозволяє прогнозувати потенційні загрози на державному кордоні, що забезпечує точними прогнозними результатами для ухвалення стратегічних рішень;

— синергія міжвідомчої взаємодії та міжнародна інтеграція (цифровізація) публічного управління є головним інструментом створення єдиного інформаційного простору. На міжнародному рівні це відкриває шлях до повної сумісності з безпековими системами ЄС та НАТО (наприклад, Eurosur або SIS), що критично важливо для процесу євроінтеграції України;

— оптимальне використання наявних ресурсів та операційна ефективність (автоматизація процесів (електронні черги, біометричний контроль)) знижує навантаження на особовий склад. У масштабах національної безпеки це означає суттєве підвищення пропускної спроможності кордонів при одночасному посиленні рівня їхньої захищеності;

— посилена увага до кібербезпеки як нового базового аспекту захисту (оптимізація управлінських рішень неможлива без розвитку архітектури кіберзахисту критичних баз даних та каналів зв'язку, відповідно сфера національної безпеки актуалізує необхідність, щоб управлінське рішення у сфері безпеки та охорони кордону розроблялося за принципом пріоритету кібернетичної стійкості (Cybersecurity by Design)).

Таким чином, цифровізація процесу управління на державному кордоні є стратегічним чинником зміцнення національної безпеки, що одночасно забезпечує підвищення економічної стабільності та захист територіальної цілісності держави. Подальший розвиток цифрових інструментів у цій сфері має ґрунтуватися на принципах інтеграції, аналітичної обґрунтованості, орієнтованості на ризики та кіберстійкості, що сукупно формують сучасну модель ефективного публічного управління у безпековій сфері. Водночас цифровізація не лише підвищує ефективність прийняття рішень у сфері прикордонної та національної безпеки, а й змінює саму природу публічного управління, трансформуючи його на гібридну систему взаємодії людини та інтелектуальних технологій.

Список використаних джерел

1. Кух С. П. Теоретико-методологічні підходи до трактування сутності цифровізації та цифрової трансформації публічної служби у сучасному науковому дискурсі. *Ефективність державного управління*. 2023. Вип. 1/2 (74/75). С. 52–56. https://doi.org/10.36930/507409.
2. Чмерук Г. Г. Цифровізація — тренд світового розвитку, який визначає розвиток економіки і суспільства. *Економічний простір*. 2020. № 153. С. 18–24. https://doi.org/10.32782/2224-6282/153-3.

unz.univer.km.ua ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98

3. Криворучко І. В. Ключові тренди цифровізації публічного управління в контексті євроінтеграції України. *Теорія та практика державного управління*. 2024. Вип. 2 (79). С. 115–135. http://doi.org/10.26565/1727-6667-2024-2-06.
4. Ненько С. С. Цифровізація публічного адміністрування як фактор модернізації адміністративно-правового забезпечення підприємництва. *Юридичний науковий електронний журнал*. 2025. № 9. С. 160–165. https://doi.org/10.32782/2524-0374/2025-9/33.
5. Шопіна І. М. Державна прикордонна служба України як суб'єкт забезпечення національної, державної, прикордонної безпеки та безпеки державного кордону. *Фаховий науковий журнал «Інтернаука». Серія: Юридичні науки*. 2022. № 10. https://doi.org/10.25313/2520-2308-2022-10-8353.
6. Ганьба О. Б. Правові відносини у сфері прикордонної безпеки України: теоретичні і прикладні проблеми. Вінниця : Твори, 2020. 448 с.
7. Прикордонна безпека України: становлення, сучасний стан, проблеми і перспективи / В. О. Назаренко, В. М. Серватюк, О. М. Ставицький та ін. Хмельницький : Вид-во НАДПСУ, 2018. 188 с. *Репозитарій НАДПСУ (IrNASBGSU)*. URL: https://t.ly/iA3VA.
8. Купрієнко Д. А. Основні поняття та категорії у сфері забезпечення прикордонної безпеки. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*. 2014. № 1 (61). С. 357–368.
9. Телюк О. В. Удосконалення механізмів реалізації державної регіональної політики на основі цифровізації. *Вісник Херсонського національного технічного університету*. 2025. № 2 (93), Ч. 1. С. 331–336. https://doi.org/10.35546/kntu2078-4481.2025.2.1.44.
10. Розділ 6. Інновації та цифровізація. Щорічний звіт Адміністрації державної прикордонної служби України для медіа і громадянського суспільства за 2025 рік (09.03.2026). *Державна прикордонна служба України*. URL: https://t.ly/Sfzwf.

Inna SHEVCHUK, Eduard SHCHEPANSKY
(Leonid Yuzkov Khmelnytskyi University of Management and Law)

Digitalisation of the Public Management System of Border Security as a Factor in Optimising Management Decisions in the Field of National Security

The article examines the role and significance of digitalisation in transforming the public management system of border security. The author substantiates that the introduction of the latest digital technologies (AI, Big Data, automated risk analysis systems) is a determining factor in optimising public management decisions. The authors emphasise that digitalisation changes the traditional cycle of management decision-making and includes the following interrelated stages: automated information collection; analytical processing and risk assessment; formation of alternative management decision options. Strengthening the use of decision support systems (Decision Support Systems, DSS) and the implementation of management decisions and monitoring results. The transition from traditional control models to data-driven management (Data-driven decision making), which allows minimising corruption risks and the human factor, is considered. Particular attention is paid to the integration of border components within a single digital space, which contributes to increasing the effectiveness of responding to hybrid threats. It has been proven that the digitalisation

ISSN 2078-9165 Університетські наукові записки, 2026, № 2 (110), С. 88-98. unz.univer.km.ua

of the management process at the border directly strengthens the national security of the state by enhancing economic stability and territorial integrity. The results of the study suggest recommendations for further improvement of digital tools in the activities of public authorities, in particular, to expand the use of artificial intelligence technologies and predictive analytics to predict the risks of cross-border crime and optimize control procedures; to strengthen the implementation of control models based on risk assessment; to ensure cybersecurity of digital border management systems; to improve digital accountability and audit systems that will ensure full transparency and traceability of management decisions and increase the level of trust in public institutions.

***Keywords**: public administration, digitalisation, management decision, border security, national security, hybrid threats, integrated border management, digital transformation, risk analysis.*

Надійшла до редакції	30.03.2026	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; Е. Щепанський — концепція дослідження, методологія, збір матеріалів, загальне керівництво дослідженням.

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. Автори статті входять 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.