Адміністративне право і процес

УДК 342.743 : 351.86

DOI https://doi.org/10.5281/zenodo.20609661

Правове регулювання та напрями вдосконалення державного управління у сфері національної безпеки

Минюк Олена Юріївна,
кандидат юридичних наук, доцент,
доцент кафедри фінансового та податкового права,
Державний податковий університет, м. Ірпінь, Україна
https://orcid.org/0009-0001-6277-6328

Низицький Ростислав Олегович,
здобувач вищої освіти другого (магістерського) рівня кафедри
фінансового та податкового права,
Державний податковий університет, м. Ірпінь, Україна
https://orcid.org/0009-0008-7684-6869

Мітла Марія Олегівна,
здобувачка вищої освіти першого (бакалаврського) рівня, Навчально-
науковий інститут права,
Державний податковий університет, м. Ірпінь, Україна
https://orcid.org/0009-0001-6466-1807

Прийнято: 16.05.2026 | Опубліковано: 30.05.2026

Анотація. У статті досліджено правове регулювання та трансформацію системи національної безпеки як складного об’єкта державного управління.

З’ясовано, що в сучасних умовах глобалізаційних процесів, посилення геополітичної нестабільності, збройної агресії проти України, гібридних, кібернетичних, інформаційних та економічних загроз важлива роль відводиться державному управлінні у сфері національної безпеки. Обгрунтовано, що традиційні методи управління не відповідають динаміці «гібридної війни на виснаження», що потребує переходу до принципів гнучкості та технологічності, удосконалення механізмів правового, стратегічного планування, координації діяльності органів державної влади, впровадження ризик-орієнтованих та проєктних підходів до управління безпековими процесами.

Метою даного дослідження є комплексне обґрунтування та аналіз існуючих управлінських підходів, розробка прикладних практичних рекомендацій, спрямованих на докорінне вдосконалення системи державного управління у сфері національної безпеки України. В умовах сучасної геополітичної нестабільності, ведення повномаштабної гібридної війни на виснаження та зростання кібернетичних й інформаційних загроз, поставлено мету трансформації наявної державно-управлінської моделі. Науковий пошук спрямований на перехід від декларативних, застарілих та бюрократизованих методів до інструментальних, гнучких і високотехнологічних алгоритмів взаємодії, що забезпечують збереження суверенітету, територіальної цілісності та сталий розвиток суспільства відповідно до європейських та євроатлантичних стандартів.

Для досягнення поставленої мети у статті застосовано комплекс загально-наукових та спеціальних методів дослідження. Методологічну основу склав системний підхід, який дозволив розглянути національну безпеку як складну, багаторівневу та міжгалузеву структуру, що поєднує воєнну, економічну, кібернетичну, інформаційну та інші підсистеми). За допомогою методів критичного, порівняльного та системно-структурного аналізу було зіставлено традиційні управлінські підходи періоду 2021-2025

 ISSN: 3041-2110

років із новітніми іноваційними концепціями. Метод моделювання та прогностичний метод було залучено під час розробки перспективних цифрових систем і триєтапного проєкту комплексної моделі.

Головним результатом дослідження є запропонований проєкт комплексної моделі підвищення ефективності національної безпеки «Smart Security Ecosystem – 2026» , який дозволить змінити саму філософію державного управління: від «утримання позицій» до «випереджального розвитку». Проєкт спрямований на створення інтегрованої, гнучкої та ефективної системи, здатної реагувати на сучасні загрози, мінімізувати ризики та забезпечувати довгострокову безпеку держави.

У висновках наголошується, що запропоновані напрями дозволять не просто покращити окремі аспекти управління, а створять нову якість державної безпеки, здійснивши перехід від пасивної стратегії «утримання позицій» до стратегії «випереджального розвитку». Автори підкреслюють, що в сучасних конфліктах XXI століття перемагає та сторона, яка швидше обробляє великі масиви інформації та ефективніше координує наявні рисурси, а не та яка має більше зброї. Реформування правового регулювання має змінитися з декларативного русла до інструментального – створення чітких, швидкодіючих алгоритмів взаємодії державних органів, які здатні оперативно реагувати на загрози в реальному часі.

Ключові слова: національна безпека, правове регулювання, держава, державне управління, блокчейн, штучний інтелект (AI), стратегічна координація, гібридна війна, інформаційні загрози, цифрова стійкість, Smart Security Ecosystem.

ISSN: 3041-2110

Legal regulation and directions for improving public administration in the sphere of national security

Olena Myniuk,
Candidate of Law, Associate Professor,
Associate Professor of the Department of Financial and Tax Law,
State Tax University, Irpin, Ukraine
https://orcid.org/0009-0001-6277-6328

Rostyslav Nyzytskyi,
second-level (master's) student of the Department of Financial and Tax Law,
State Tax University, Irpin, Ukraine
https://orcid.org/0009-0008-7684-6869

Maria Mitla,
a student of higher education of the first (bachelor's) level, Educational and Scientific Institute of Law,
State Tax University, Irpin, Ukraine
https://orcid.org/0009-0001-6466-1807

Abstract. The article examines the legal regulation and transformation of the national security system as a complex object of public administration. It is established that under current conditions of globalization, intensifying geopolitical instability, armed aggression against Ukraine, as well as hybrid, cyber, informational, and economic threats, public administration in the field of national security plays a vital role. The study substantiates that traditional management methods fail to keep pace with the dynamics of a «hybrid war of attrition». This necessitates a transition toward the principles of flexibility and technological advancement, alongside the refinement of legal and strategic planning mechanisms,

 ISSN: 3041-2110

improved coordination among state authorities, and the implementation of risk-oriented and project-based approaches to managing security processes.

The purpose of this study is to provide a comprehensive substantiation and analysis of existing management approaches, as well as to develop applied, practical recommendations aimed at fundamentally improving the public administration system within Ukraine's national security sector. Amidst current geopolitical instability, an ongoing full-scale hybrid war of attrition, and escalating cyber and informational threats, the study aims to transform the existing state management model. This scholarly inquiry focuses on shifting from declarative, outdated, and bureaucratic methods toward instrumental, agile, and high-tech interaction algorithms that ensure the preservation of sovereignty, territorial integrity, and the sustainable development of society in alignment with European and Euro-Atlantic standards.

To achieve this purpose, the article employs a comprehensive set of general scientific and specialized research methods. The methodological foundation is rooted in a systems approach, which allows for the examination of national security as a complex, multi-tiered, and cross-sectoral structure integrating military, economic, cyber, informational, and other subsystems. Through the methods of critical, comparative, and systemic-structural analysis, traditional management approaches from the 2021–2025 period are contrasted with cutting-edge innovative concepts. Modeling and forecasting methods are further utilized to develop promising digital systems and a three-stage project for a comprehensive model.

The primary result of this research is the proposed project for a comprehensive model to enhance national security efficiency, titled the «Smart Security Ecosystem – 2026». This framework shifts the very philosophy of public administration from «holding ground» to «anticipatory development». The project is designed to establish an integrated, flexible, and resilient system capable of responding to contemporary threats, mitigating risks, and ensuring the long-term security of the state.

 ISSN: 3041-2110

The conclusions emphasize that the proposed pathways will do more than merely improve isolated aspects of management; they will forge a new caliber of state security by transitioning from a passive strategy of «holding ground» to one of «anticipatory development». The authors highlight that in modern 21st-century conflicts, victory belongs not to the side with more weapons, but to the one that processes vast arrays of information faster and coordinates available resources more efficiently. The reform of legal regulation must pivot from a declarative course to an instrumental one - focusing on creating clear, high-speed algorithms for interaction among state bodies that can promptly counter threats in real time.

Keywords: national security, legal regulation, state, public administration, blockchain, artificial intelligence (AI), strategic coordination, hybrid warfare, information threats, digital resilience, Smart Security Ecosystem.

Постановка проблеми. Національна безпека є однією з ключових сфер життєдіяльності держави, від ефективності якої залежить збереження суверенітету, територіальної цілісності, конституційного ладу та сталого розвитку суспільства. В умовах сучасних глобалізаційних процесів, посилення геополітичної нестабільності, збройної агресії проти України, гібридних, кібернетичних, інформаційних та економічних загроз значно зростає роль державного управління у сфері національної безпеки.

Сучасні виклики вимагають не лише адекватного реагування з боку сектору безпеки і оборони, а й необхідністю адаптації національної системи безпеки до європейських та євроатлантичних стандартів державного управління. У зв'язку з цим дослідження проблем і перспектив розвитку державного управління у сфері національної безпеки є науково обґрунтованим, своєчасним і практично значущим.

Аналіз останніх досліджень і публікацій. Проаналізувавши дослідження вітчизняних науковців, таких як В. Базиченко [1], В. Горбулін [2; 3], Я. Конопля [4], Е. Лібанова [5], О. Пархоменко-Куцевіл [6], О. Рєзнікова

[7], Д. Сергієнко [8], М. Сироватченко [9], О. Сокол [10] та С. Ядуха [11], ми виокремили основні проблеми у цій сфері. Водночас, попри наявність значної кількості наукових досліджень, недостатньо опрацьованими залишаються питання комплексного поєднання теоретико-методологічних засад державного управління з практичними аспектами реалізації державної політики у сфері національної безпеки, а також розробки прикладних управлінських моделей, що зумовлює необхідність подальших наукових пошуків у зазначеному напрямі.

Виділення невирішених раніше частин загальної проблеми. На основі проведеного аналізу стає очевидним, що традиційні методи державного управління не встигають за динамікою «гібридної війни на виснаження». Стратегічне вдосконалення системи нацбезпеки у 2026 р. та на подальшу перспективу має базуватися на принципах гнучкості, технологічності та національної стійкості. Запропонований проєкт «Smart Security Ecosystem – 2026» не просто покращить окремі аспекти управління, а допоможе створити нову якість державної безпеки.

Постановка завдання. Метою статті є - теоретичне обґрунтування та розробка практичних рекомендацій щодо вдосконалення державного управління у сфері національної безпеки України. Для досягнення поставленої мети передбачено розвязання таких завдань:

– виявити основні проблеми та недоліки державного управління у сфері національної безпеки;

– обґрунтувати напрями та розробити проєктні пропозиції щодо вдосконалення механізмів державного управління у цій сфері.

Виклад основного матеріалу. Як об’єкт державного управління національна безпека характеризується складною внутрішньою структурою, багаторівневістю та міжгалузевим характером. Вона включає сукупність взаємопов’язаних підсистем, зокрема воєнну, політичну, соціальну, економічну, кібернетичну, інформаційну, екологічну та гуманітарну безпеку.

ISSN: 3041-2110

Кожна з цих складових має власні загрози, інструменти забезпечення та відповідних суб'єктів управлінського впливу, що зумовлює необхідність координації дій органів державної влади.

У Стратегії національної безпеки України зазначено, що найвищим пріоритетом держави є встановлення миру та відновлення суверенітету й територіальної цілісності країни у межах міжнародно визнаних кордонів. [12].

В. Хаустова, Н. Трушкіна [13] та В. Шевчук [14] наголошують, що глобальні індекси безпеки, стійкості, державного управління, кібербезпеки та миру дозволяють не лише визначити місце України у світовій системі безпеки, а й виявити ключові вразливості, які потребують першочергового державного реагування.

У цьому контексті доцільним є вдосконалення ключових механізмів державного управління з урахуванням інноваційних управлінських підходів і новітніх технологій. Новітні інформаційні технології стали системоутворювальним чинником сучасних службово-бойових дій, істотно збільшуючи інформаційне навантаження на органи управління.

За даними світової практики, обсяг інформації, що створюється та використовується у глобальному суспільстві, щорічно зростає в середньому на 57 % [15, с. 9] Інформаційні технології охоплюють комплекс засобів і систем для створення, зберігання, обміну та обробки інформації. Сучасні загрози мають гібридний характер, тому правове поле потребує розширення і на віртуальний простір.

1. Створення постійно діючого Міжвідомчого центру стратегічної координації безпеки (МЦСКБ) при РНБО України (рис.1.1), який виконуватиме функції координації, аналізу та стратегічного прогнозування загроз. Подібні центри функціонують у США (National Security Council Staff) та Ізраїлі (National Security Council), де вони забезпечують інтеграцію військових, економічних, кібер- та гуманітарних аспектів безпеки в єдину систему управління. Центр виступає «єдиним вікном» для агрегації інформації

від розвідки, МВС, Міненерго та Міністерства культури і стратегічних комунікацій. МЦСКБ працює за принципом «Hot-Swap Management» (гаряча заміна пріоритетів) – він миттєво перемикає ресурси держави на ту ділянку, де виникла критична загроза (наприклад, з військового фронту на енергетичний чи ідеологічний).

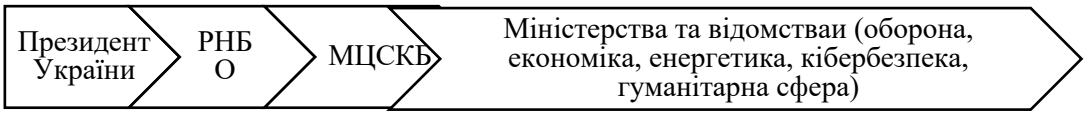

Рис. 1.1. Організаційна схема міжвідомчої координації у сфері нацбезпеки

2. Створення системи предиктивного аналізу «Sentinel-AI» на базі Big Data – для подолання суб'єктивізму та інертності аналітичних звітів пропонується впровадження системи інтелектуального прогнозування (рис.1.2). Використання великих масивів даних (Big Data) – від супутникових знімків та показників датчиків на об'єктах критичної інфраструктури до фінансових транзакцій та активності в інфосфері. Алгоритми AI проводять кореляційний аналіз (шукають зв'язки між подіями, які непомітні людині). Наприклад, система може виявити підготовку до ворожої операції за непрямими ознаками: синхронним розповсюдженням фейків у соціальних мережах та аномальними кібератаками на логістичні вузли.

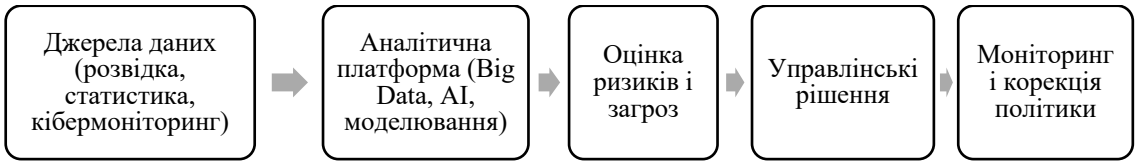

Рис. 1.2. Блок-схема інформаційно-аналітичного забезпечення управління національною безпекою

Створення МЦСКБ забезпечить необхідну «вертикаль» управління, тоді як використання Big Data та AI надасть цій вертикалі «зір» та здатність до передбачення. Це дозволить державі випереджати кроки агресора, діючи не лише симетрично на полі бою, а й асиметрично в управлінському та інформаційному просторах (табл.1.1).

Таблиця 1.1

Функціональні можливості нових механізмів

Пропозиція	Технологічний стек	Управлінський ефект
МЦСКБ при РНБО	Комунікаційні шини безпеки, CRM-системи управління завданнями.	Ліквідація «відомчого егоїзму», прискорення реакції на 300%.
Sentinel-AI (Big Data)	Нейромережі, кластерні обчислення, хмарна аналітика.	Перехід від констатації фактів до прогнозування загроз за 48–72 години до їх настання.

3. Створення «Центру управління стійкістю» (Resilience Hub) – замість розрізнених відомчих департаментів пропонується створити єдину крос-функціональну платформу для синхронізації дій військових та цивільних адміністрацій. Законодавче спрощення процедури передачі управлінських функцій від цивільних органів влади до військових адміністрацій сприятиме оптимізації делегування повноважень, особливо на деокупованих та прифронтових територіях. Впровадження матричної структури управління, де для кожного типу загрози (військова, політична, економічна, енергетична, інфраструктурна) призначається тимчасовий «Task Force» (цільова група) з повноваженнями залучати ресурси різних міністерств.

4. Впровадження технології «Цифрового двійника національної безпеки» (Digital Twin of National Security) – створення віртуальної моделі критичної інфраструктури, логістики та демографічних потоків України є найбільш перспективною технологією для прогнозування наслідків управлінських рішень. Використання ШІ (AI) для моделювання сценаріїв: «Що станеться, якщо...». Наприклад, моделювання навантаження на енергосистему при відключенні конкретного вузла або розрахунок темпів мобілізації кадрів для відновлення зруйнованої інфраструктури.

5. Платформа «Linguo-Shield» (інформаційно-ідеологічний механізм) – для протидії роботі російських ботів і фейків, «наказам» РПЦ та іншим гібридним ідеологічним атакам пропонується використовувати новітні NLP-технології (обробка природної мови), що передбачає автоматизований

моніторинг медійного простору на предмет виявлення наративів, що загрожують нацбезпеці. AI-алгоритми ідентифікують приховані заклики до колабораціонізму або деструктивного впливу ще на етапі їх зародження.

Для наочності порівняємо ці механізми управління з більш традиційними для України (табл.1.2).

Таблиця 1.2

Порівняння традиційних та запропонованих механізмів управління

Механізм	Традиційний підхід (2020-2024)	Пропонований інноваційний підхід (з 2026)
Прийняття рішень	На основі звітів та паперових доповідей	Real-time Data (на основі даних з сенсорів, супутників та AI-аналітики)
Координація	Відомчі листування, наради	Blockchain-протоколи (автоматичне виконання смарт-контрактів між відомствами)
Оборонні закупівлі	Закриті тендери з високим ризиком корупції	Tokenization (прозорий облік ресурсів через блокчейн-реєстри без розкриття секретних даних)
Кіберзахист	Реактивне виправлення вразливостей	Predictive Defense (превентивне блокування атак за допомогою нейромереж)

6. Хмарна архітектура «GovCloud-Security» – перенесення критичних державних реєстрів та систем управління на децентралізовані хмарні сервери, розподілені по країнах-партнерах НАТО, що унеможливлює фізичне знищення «мізків» державного управління ракетними ударами по Києву чи інших центрах.

7. Механізм «Громадянської стійкості» (застосунок «Оборона-ID») – гейміфікація та цифровізація цивільного захисту. Громадяни через застосунок отримують не лише сповіщення, а й конкретні завдання (наприклад, перевірка сховища, оновлення запасів води), за виконання яких отримують соціальні бали або пільги.

Також варто відзначити, що важливою складовою удосконалення інституційного та організаційного механізмів є впровадження принципу безперервного управління, що ґрунтується на постійному циклі підготовки та

прийняття управлінських рішень. Процес управління у сфері національної безпеки має розглядатися як динамічна система, що включає безперервний збір і аналіз інформації, оцінку безпекової обстановки, формування управлінських рішень, постановку завдань виконавцям і контроль їх виконання з подальшим коригуванням дій (рис.1.3). У межах такого підходу управління та прийняття рішень є взаємопов'язаними елементами єдиного процесу, а кожне управлінське рішення повинно супроводжуватися чітким визначенням завдань, ресурсів, термінів та відповідальних суб'єктів, що забезпечує його практичну реалізацію та адаптацію до змін безпекового середовища.

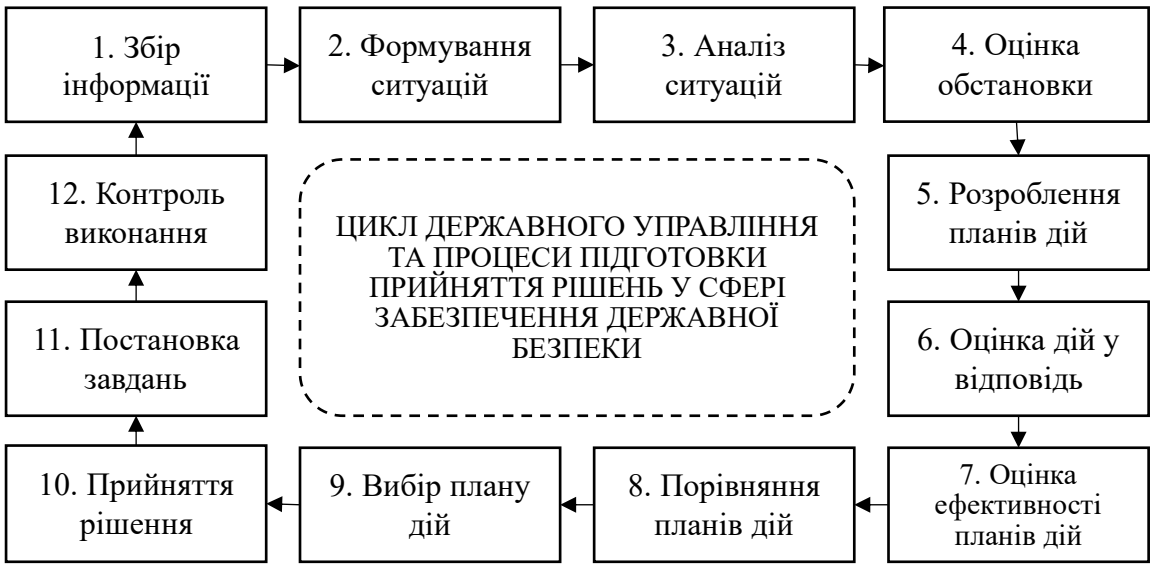

Рис. 1.3. Безперервний цикл державного управління та процеси підготовки прийняття рішень у сфері забезпечення державної безпеки

На основі стратегічних напрямів та запропонованих механізмів пропонується проект створення Комплексної екосистеми «Smart Security Ecosystem – 2026». Метою проекту є перехід від фрагментарного управління до цілісної, цифровізованої системи національної стійкості.

Проєкт розрахований на 18 місяців і реалізується у три етапи:

ISSN: 3041-2110

I. Інституційне злиття (1–6 місяць) – формування МЦСК при РНБО. Призначення офіцерів зв'язку (liaison officers) від кожного міністерства.

II. Технологічна інтеграція (7–12 місяць) – запуск платформи «Sentinel-AI». Об'єднання державних реєстрів у захищену хмарну мережу «GovCloud-Security».

III. Громадянська імплементація (13–18 місяць) – масштабування застосунку «Оборона-ID» на всю країну та підключення територіальних громад до «Цифрового двійника».

Проект базується на взаємодії трьох ключових контурів управління (рис. 1.4)

Рис. 1.4. Функціональна модель проекту

Ключовими компонентами моделі є наступні:

– модуль предиктивної безпеки (AI-Predictive Module) – центральний елемент проекту, що використовує Big Data для створення «Теплової карти загроз». Система автоматично аналізує ризики у всіх сферах (від воєнної до екологічної) і видає рекомендації щодо перерозподілу ресурсів;

– система «Прозорий ресурс» (Blockchain Resource Control) – механізм управління оборонним бюджетом та міжнародною допомогою через технологію блокчейн. Це дозволяє в реальному часі відстежувати кожну одиницю допомоги від кордону до кінцевого споживача, ліквідуючи корупційні ризики та підвищуючи довіру партнерів;

– координаційна матриця «Resilience Matrix» – алгоритм швидкого реагування, який автоматично формує план дій для громад у разі надзвичайної

ситуації (наприклад, пошкодження ТЕС). Матриця прораховує логістику підвезення води, розгортання мобільної генерації та канали інформування населення (табл. 1.3).

Таблиця 1.3

Детальна архітектура та план реалізації проєкту «Smart Security Ecosystem – 2026»

Параметр проєкту	**Опис та функціональний зміст**	**Інструментарій та новітні технології**	**Прикладний кейс (застосування)**	**Етап впровадження**
1	2	3	4	5
1. Когнітивний контур (аналітика)	Автоматизований збір та аналіз Big Data для виявлення прихованих патернів загроз.	Sentinel-AI: нейромережі архітектури Transformer; Palantir Foundry для інтеграції розрізнених даних.	Передбачення дестабілізації в регіоні через аналіз аномальних сплесків активності в ботофермах рф та рухів капіталу.	І етап (1-4 міс.) – навчання моделей на історичних даних.
2. Інституційний контур (координація)	Створення Міжвідомчого центру (МЦСКБ) як «ситуаційної кімнати» вищого рівня при РНБО.	Real-time Collaboration Suites: захищені крипто-канали зв'язку; Jira Enterprise для трекінгу безпекових завдань.	Синхронізація дій ДСНС, Міненерго та ЗСУ протягом 5 хвилин після масованого комбінованого удару по інфраструктурі.	І етап (2-5 міс.) – формування штату та протоколів взаємодії.
3. Ресурсний контур (контроль)	Тотальний моніторинг використання оборонних коштів та міжнародної військової допомоги.	Hyperledger Fabric (Blockchain): розподілений реєстр для обліку активів; Smart-contracts для автоматичних виплат постачальникам.	Можливість для західного донора побачити шлях кожного виділеного долара або снаряда до конкретної бригади без розкриття дислокації.	ІІ етап (6-12 міс.) – оцифрування складських залишків та логістики.
4. Ідеологічний контур (захист)	Протидія гібридним релігійним та культурним операціям впливу.	Linguo-Shield (NLP): алгоритми обробки мови для детекції мови ворожнечі	Автоматичне виявлення мережі агентів впливу, що поширюють ворожі наративи через закриті	ІІ етап (8-14 міс.) – інтеграція з медіа-моніторингом.

ISSN: 3041-2110

		та наративів «русского міра».	чати соціальних мереж.	
5. Цивільний контур (стійкість)	Цифрова взаємодія держави з громадянином у питаннях оборони та цивільного захисту.	SuperApp «Оборона-ID»: мікросервісна архітектура; технологія Edge Computing для роботи в умовах відсутності інтернету.	Громадянин отримує QR-код на доступ до укриття або стає частиною «цифрової ТрО», фіксуючи проліт БПЛА через смартфон.	III етап (12-18 міс.) – масове тестування та запуск.
6. Модель виживання (інфраструктура)	Забезпечення життєздатності системи управління при фізичному знищенні центрів.	Decentralized GovCloud: хмарні сервери в дата-центрах країн НАТО; Starlink 3.0 для безперебійного каналу управління.	Перенесення всього державного апарату у «хмару» протягом 1 хвилини у разі загрози захоплення або знищення адміністративних будівель.	I-III етапи (постійно) – нарощування хмарних потужностей.

Висновки. Таким чином, запропоновані напрями спрямовані на створення інтегрованої, гнучкої та ефективної системи, яка здатна реагувати на сучасні загрози, мінімізувати ризики та забезпечувати довгострокову безпеку держави. Вони формують основу для подальшої розробки конкретних механізмів удосконалення управління та проєкту комплексної моделі підвищення ефективності національної безпеки, а також дозволяють змінити саму філософію державного управління: від «утримання позицій» до «випереджального розвитку». Проєкт «Smart Security Ecosystem – 2026» не просто покращує окремі аспекти управління, а створює нову якість державної безпеки. Це відповідь на виклики XXI століття, де перемагає не лише той, хто має більше зброї, а той, хто швидше обробляє інформацію та ефективніше координує наявні ресурси. Правове вдосконалення державного управління у цій сфері має зміститися від декларативного характеру (загальних гасел у законах) до інструментального – створення чітких, швидкодіючих алгоритмів

взаємодії державних органів, які здатні оперативно реагувати на загрози в реальному часі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Базиченко В. Проблеми та перспективи державного управління у сфері національної безпеки та оборони держави. *Публічне управління та адміністрування в Україні: євроінтеграційний поступ* : матеріали Всеукраїнської науково-практичної конференції за міжнародною участю (Івано-Франківськ, 31 травня 2024 р.). Івано-Франківськ : ІФНТУНГ, 2024. С. 317-319.

2. Горбулін В. П. Мій шлях у задзеркалля: нотатки на берегах історії. Київ : Брайт Букс, 2024. 312 с.

3. Горбулін В. П. Світова гібридна війна: український фронт : Монографія. Харків : Фоліо, 2020. 496 с.

4. Конопля Я., Шевчук В. Концептуалізація публічного управління національною безпекою: від менеджеризму до оборонного менеджменту. *Геополітика України: історія і сучасність* : Збірник наукових праць. 2025. № 1 (34). С. 126-133.

5. Лібанова Е. «Бебі-буму після війни не буде»: інтерв'ю Лібанової про міграцію, кризу кадрів і настрої українців / РБК-України (2025). *URL*: https://www.rbc.ua/rus/news/bebi-bumu-pislya-viyni-bude-interv-yu-libanovoyi-1764248884.html

6. Пархоменко-Куцевіл О. Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти*. 2023. № 3. С. 143-150.

7. Резнікова О. Національна стійкість в умовах мінливого безпекового середовища : Монографія. Київ : НІСД, 2022. 456 с.

 ISSN: 3041-2110

8. Сергієнко Д., Бикова А. Національна безпека України в умовах війни. *Матеріали конференцій МЦНД* (20 червня 2025 р., м. Чернігів). 2025. С. 166-169.

9. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка»*. 2024. № 1 (41). С. 314-320.

10. Сокол О. Р. Національна безпека України в умовах її політичної трансформації крізь призму адміністративно-правових засад. *Науковий вісник Львівського державного університету внутрішніх справ*. 2025. № 3. С. 86-94.

11. Ядуха С. Й., Лисак О. М. Національна безпека України. Її основні аспекти, принципи та загрози. *Вісник Хмельницького національного університету*. 2018. № 5 (1). С. 131-136.

12. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

13. Хаустова В., Трушкіна Н. Оцінка стану національної безпеки України у світових індексах і рейтингах. XVIII Міжнародна науково-практична конференція «Моделювання та прогнозування економічних процесів». 2024. Т. 18, № 1. С. 127-130.

14. Шевчук В. Рейтингування стану національної безпеки держави: підходи до стратегування. *Проблеми і перспективи економіки та управління*. 2025. № 2 (42). С. 50-60.

15. Споришев К. О. Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України: теорія, методологія, практика : монографія. Одеса : Олді+, 2024. 314 с.

 ISSN: 3041-2110