МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗВО «ВІДКРИТИЙ МІЖНАРОДНИЙ УНІВЕРСИТЕТ РОЗВИТКУ ЛЮДИНИ «УКРАЇНА»

Кваліфікаційна наукова
праця на правах рукопису

ПУСТОВІТ ЯРОСЛАВ БОРИСОВИЧ

УДК 351.86:004.8:355.02](477)

ДИСЕРТАЦІЯ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПІДВИЩЕННІ ОБОРОНОЗДАТНОСТІ УКРАЇНИ: АСПЕКТ ПУБЛІЧНОГО УПРАВЛІННЯ

281 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ **Пустовіт Я.Б.**

Науковий керівник
ФОРОСТОВЕЦЬ АЛЬОНА СЕРГІЇВНА,
доктор філософії з галузі знань «Управління та адміністрування»,
доцент

Київ – 2026

АНОТАЦІЯ

Пустовіт Я.Б. Використання штучного інтелекту в підвищенні обороноздатності України: аспект публічного управління. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». ЗВО «Відкритий міжнародний університет розвитку людини «Україна». Київ, 2026.

У дисертаційному дослідженні здійснено теоретичне узагальнення та запропоновано науково-практичні підходи до вдосконалення публічного управління використання штучного інтелекту в підвищенні обороноздатності України.

Систематизовано вітчизняні й зарубіжні наукові підходи до визначення сутності штучного інтелекту, уточнено його співвідношення із суміжними технологічними категоріями та конкретизовано основні технологічні, функціональні й системні характеристики на основі історичного та компаративного аналізу. Обґрунтовано, що в контексті публічного управління штучний інтелект доцільно розглядати як інструмент інформаційно-аналітичного забезпечення, прогнозування, планування та підтримки прийняття управлінських рішень, використання якого сприяє посиленню інституційної спроможності держави.

Розкрито сутність обороноздатності держави як комплексного об’єкта публічного управління в системі національної безпеки, формування та розвиток якого забезпечуються взаємодією військових, економічних, технологічних, інформаційних, кадрових та організаційно-управлінських складових. За результатами історико-ретроспективного аналізу виокремлено п’ять етапів становлення обороноздатності України, що відображають еволюцію управлінських підходів від формування нормативно-інституційних засад оборони до розвитку комплексного й адаптивного управління оборонними

ресурсами та спроможностями. Уточнено зміст категорії «забезпечення обороноздатності держави» як безперервного процесу цілеспрямованої діяльності уповноважених суб'єктів щодо формування, підтримання, розвитку та реалізації оборонного потенціалу й оборонних спроможностей відповідно до пріоритетів державної політики у сфері національної безпеки і оборони. Розмежовано поняття «оборона», «обороноздатність», «оборонний потенціал», «оборонні спроможності» та «забезпечення обороноздатності», що дозволило конкретизувати роль публічного управління у формуванні та розвитку обороноздатності держави.

Обґрунтовано інтегрувальну роль публічно-управлінського узгодження у процесі перетворення оборонного потенціалу на оборонні спроможності. Визначено взаємозв'язок основних складових управлінського процесу забезпечення обороноздатності держави, зокрема оцінювання безпекових загроз, визначення оборонних потреб, мобілізації та розподілу ресурсів, координації діяльності уповноважених суб'єктів, розвитку оборонних спроможностей і коригування управлінських рішень на основі зворотного зв'язку. Доведено, що результативність забезпечення обороноздатності залежить не лише від наявності відповідного оборонного потенціалу, а й від спроможності системи публічного управління забезпечувати узгодженість, послідовність та адаптивність управлінських дій.

Систематизовано теоретичні підходи до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони, серед яких виокремлено інструментальний, аналітико-прогностичний, інституційно-управлінський, ризик-орієнтований та адаптивний підходи. На цій основі обґрунтовано п'ять взаємопов'язаних функціональних напрямів застосування штучного інтелекту в публічному управлінні забезпеченням обороноздатності держави: інформаційно-аналітичний, прогностичний, планувально-ресурсний, координаційний та контрольно-моніторинговий. Встановлено, що використання технологій штучного інтелекту за зазначеними напрямами створює передумови для підвищення обґрунтованості управлінських рішень, удосконалення

оборонного планування, оптимізації ресурсного забезпечення, посилення міжвідомчої координації та розвитку оборонних спроможностей. Аргументовано, що вплив штучного інтелекту на підвищення обороноздатності держави має переважно опосередкований характер і реалізується через вдосконалення управлінських процесів за умови належного інституційного забезпечення, управління ризиками, збереження людського контролю та відповідальності за прийняття управлінських рішень.

Проаналізовано нормативно-правові засади використання штучного інтелекту для підвищення обороноздатності України. Встановлено, що чинні стратегічні та програмні документи формують загальні політико-правові передумови розвитку технологій штучного інтелекту, проте не забезпечують комплексного правового регулювання особливостей їх розроблення, впровадження та застосування в оборонній сфері. Виявлено нормативно-правові прогалини, пов’язані з відсутністю спеціалізованого галузевого регулювання, недостатньою визначеністю правового статусу автономних і напівавтономних систем озброєння, рівнів людського контролю, критичних функцій таких систем та процедур оцінювання правомірності їх використання. Обґрунтовано необхідність удосконалення нормативно-правового забезпечення впровадження штучного інтелекту в секторі безпеки і оборони з урахуванням міжнародних стандартів, оборонних потреб держави та необхідності недопущення надмірних адміністративних обмежень, здатних уповільнювати технологічні інновації.

Визначено пріоритетні напрями вдосконалення правового регулювання використання штучного інтелекту в оборонній сфері України, зокрема уточнення понятійно-категоріального апарату, нормативного визначення автономних і напівавтономних систем озброєння та рівнів людського контролю, розроблення галузевої концепції або стратегії застосування штучного інтелекту в секторі безпеки і оборони. Обґрунтовано доцільність закріплення принципів законності, відповідальності, пояснюваності, надійності, керованості та мінімізації упередженості під час розроблення і використання відповідних технологій. Запропоновано вдосконалити організаційно-правові засади оцінювання нових

засобів і методів ведення війни, зокрема систем штучного інтелекту, шляхом визначення уповноважених суб'єктів, критеріїв і процедур проведення відповідної правової оцінки.

Досліджено інституційно-організаційні засади публічного управління використання штучного інтелекту для підвищення обороноздатності України. Встановлено, що взаємодія суб'єктів публічного управління здійснюється через систему вертикальних і горизонтальних зв'язків, які забезпечують розподіл повноважень, стратегічне керівництво, міжвідомчу координацію, інформаційний обмін та спільну інноваційну діяльність. Запропоновано функціональну систематизацію інституційної архітектури публічного управління використання штучного інтелекту в оборонній сфері за п'ятьма взаємопов'язаними блоками: політико-законодавчим, виконавчо-координаційним, безпеково-інфраструктурним, оперативно-застосовним та інноваційно-технологічним. Визначено важливість освітньо-кадрового забезпечення як необхідної умови функціонування зазначеної системи, що передбачає підготовку військових фахівців, операторів інтелектуальних систем, аналітиків, розробників оборонних технологій та фахівців із публічного управління.

Узагальнено зарубіжний досвід публічного управління використання штучного інтелекту для підвищення обороноздатності держави. Встановлено, що особливості впровадження відповідних технологій визначаються не лише рівнем технологічного розвитку, а й характером інституційної організації, стратегічної координації, ресурсного забезпечення та взаємодії державних і недержавних суб'єктів оборонно-інноваційної діяльності. Систематизовано п'ять домінантних управлінських підходів, що застосовуються в зарубіжній практиці: стратегічно-координаційний, інституційно-організаційний, централізовано-інституційний, ресурсно-адаптивний та партнерсько-інноваційний. Обґрунтовано напрями вибіркової адаптації зарубіжного досвіду до національних умов, орієнтовані на вдосконалення організаційної координації, процедур апробації та впровадження інтелектуальних технологій, кадрового забезпечення, партнерської взаємодії, управління ризиками й забезпечення

технологічної стійкості. Визначено, що використання зарубіжних управлінських практик має здійснюватися з урахуванням оборонних пріоритетів України, особливостей її інституційного середовища, ресурсних можливостей і безпекових обмежень.

Систематизовано основні проблеми публічного управління використання штучного інтелекту для підвищення обороноздатності України та встановлено їх взаємозалежний характер. Удосконалено науково-методичний підхід до оптимізації відповідних управлінських процесів, що передбачає систематизацію проблем і механізмів їх вирішення, визначення критеріїв пріоритетності управлінського реагування, диференційований добір інструментів оптимізації та оцінювання результативності їх застосування за відповідними показниками. Особливістю запропонованого підходу є поєднання проблемної орієнтації управлінського впливу з його адаптивністю, що забезпечує можливість перегляду пріоритетів, механізмів та інструментів управління відповідно до змін безпекового середовища, оборонних потреб і фактичних результатів використання технологій штучного інтелекту.

Обґрунтовано, що реалізація проблемно-адаптивного підходу передбачає безперервний взаємозв’язок між виявленням управлінських проблем, визначенням пріоритетів їх вирішення, добором відповідних механізмів, реалізацією управлінських заходів та оцінюванням отриманих результатів. При цьому оцінювання результативності розглядається не лише як завершальна стадія управлінського процесу, а й як інструмент зворотного зв’язку, що забезпечує своєчасне виявлення нових проблем, уточнення причин їх виникнення та коригування управлінських рішень. Доведено, що застосування зазначеного підходу створює передумови для підвищення обґрунтованості управлінських рішень, зменшення організаційної фрагментарності, раціонального використання ресурсів, удосконалення контролю за впровадженням інтелектуальних технологій та посилення адаптивності системи публічного управління до змін оборонних потреб держави.

Результати дисертаційного дослідження спрямовані на розвиток теоретичних положень і вдосконалення науково-методичних засад публічного управління використанням штучного інтелекту для підвищення обороноздатності України. Сформульовані положення та практичні рекомендації можуть бути використані для вдосконалення нормативно-правового й інституційно-організаційного забезпечення впровадження штучного інтелекту в обороноздатність держави, розвитку міжвідомчої взаємодії, підвищення ефективності оборонного планування та вдосконалення управлінських процесів в умовах динамічних безпекових викликів.

Ключові слова: державне управління, штучний інтелект, обороноздатність держави, публічне управління, оборона, національна безпека, публічна влада, загрози, державна політика, оборонні системи, стратегічні рішення, цифрові технології, цифрова трансформація, цифровізація, сектор безпеки і оборони.

ANNOTATION

Pustovit Ya. B. The Use of Artificial Intelligence to Enhance Ukraine's Defense Capabilities: A Public Administration Perspective. – The qualification scientific work on the rights of manuscript.

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 28 "Public Management and Administration", in the specialty 281 "Public Management and Administration". HEI "Open International University of Human Development "Ukraine". Kyiv, 2026.

The dissertation provides a theoretical synthesis and proposes scientific and practical approaches to improving public administration of the use of artificial intelligence to enhance Ukraine's defense capabilities.

Based on historical and comparative analysis, Ukrainian and international scholarly approaches to defining the nature of artificial intelligence have been systematized, its relationship with related technological concepts has been clarified, and its principal technological, functional, and systemic characteristics have been specified. It has been substantiated that, in the context of public administration, artificial intelligence should be regarded as a tool for information and analytical support, forecasting, planning, and decision-making support, the application of which contributes to strengthening the institutional capacity of the state.

The nature of national defense capability as a complex object of public administration within the national security system has been examined. Its formation and development are ensured through the interaction of military, economic, technological, informational, human resource, and organizational and administrative components. Based on historical and retrospective analysis, five stages in the development of Ukraine's defense capabilities have been identified, reflecting the evolution of public administration approaches from the establishment of legal and institutional foundations of defense to the development of comprehensive and adaptive management of defense resources and capabilities. The concept of "ensuring national defense capability" has been further clarified as a continuous process of purposeful

activities undertaken by authorized entities to establish, maintain, develop, and utilize defense potential and defense capabilities in accordance with national security and defense policy priorities. A distinction has been made between the concepts of "defense," "defense capability," "defense potential," "defense capabilities," and "ensuring defense capability," thereby specifying the role of public administration in strengthening and developing the state's defense capabilities.

The integrative role of coordination within public administration in transforming defense potential into defense capabilities has been substantiated. The interrelationships among the principal components of the public administration process aimed at ensuring national defense capability have been identified, including security threat assessment, identification of defense requirements, mobilization and allocation of resources, coordination among authorized entities, development of defense capabilities, and adjustment of administrative decisions through feedback mechanisms. It has been demonstrated that the effectiveness of efforts to ensure defense capability depends not only on the availability of adequate defense potential but also on the ability of the public administration system to ensure the coherence, consistency, and adaptability of administrative actions.

Theoretical approaches to the use of artificial intelligence in public administration of the security and defense sector have been systematized, with five principal approaches identified: instrumental, analytical and predictive, institutional and administrative, risk-oriented, and adaptive. On this basis, five interconnected functional areas of artificial intelligence application in public administration for ensuring national defense capability have been substantiated: information and analytical support, forecasting, planning and resource management, coordination, and control and monitoring. It has been established that the application of artificial intelligence technologies in these areas creates opportunities to improve the justification of administrative decisions, enhance defense planning, optimize resource allocation, strengthen interagency coordination, and develop defense capabilities. It has been argued that the contribution of artificial intelligence to enhancing national defense capability is predominantly indirect, operating through improvements in public

administration processes, provided that appropriate institutional arrangements, risk management mechanisms, human oversight, and accountability for administrative decisions are maintained.

The legal and regulatory foundations governing the use of artificial intelligence to enhance Ukraine's defense capabilities have been analyzed. It has been established that existing strategic and policy documents provide a general political and legal framework for the development of artificial intelligence technologies but do not ensure comprehensive regulation of their development, implementation, and application in the defense sector. Regulatory gaps have been identified, including the absence of specialized sector-specific regulation, insufficient legal clarity regarding the status of autonomous and semi-autonomous weapon systems, levels of human control, the critical functions of such systems, and procedures for assessing the legality of their use. The need to improve the legal and regulatory framework for artificial intelligence implementation in the security and defense sector has been substantiated, taking into account international standards, national defense requirements, and the importance of avoiding excessive administrative restrictions that could hinder technological innovation.

Priority directions for improving the legal regulation of artificial intelligence applications in Ukraine's defense sector have been identified. These include refining the conceptual and terminological framework, establishing legal definitions of autonomous and semi-autonomous weapon systems and levels of human control, and developing a sector-specific concept or strategy for artificial intelligence applications in the security and defense sector. The importance of incorporating the principles of legality, accountability, explainability, reliability, controllability, and bias mitigation into the development and deployment of relevant technologies has been substantiated. Improvements to the organizational and legal framework for reviewing new means and methods of warfare, including artificial intelligence systems, have been proposed through the designation of competent authorities and the establishment of appropriate criteria and procedures for conducting legal assessments.

The institutional and organizational foundations of public administration

concerning the use of artificial intelligence to enhance Ukraine's defense capabilities have been examined. It has been established that interaction among public administration actors is structured through vertical and horizontal relationships that facilitate the distribution of powers and responsibilities, strategic leadership, interagency coordination, information exchange, and collaborative innovation. A functional classification of the institutional architecture of public administration governing artificial intelligence applications in the defense sector has been proposed, comprising five interconnected components: political and legislative, executive and coordination, security and infrastructure, operational and application, and innovation and technology. The importance of education and human resource development has been emphasized as an essential prerequisite for the effective functioning of this system, including the training of military personnel, intelligent system operators, analysts, defense technology developers, and public administration professionals.

International experience in public administration of artificial intelligence applications aimed at enhancing national defense capabilities has been synthesized. It has been established that the specific characteristics of implementing these technologies are determined not only by a country's level of technological development but also by its institutional arrangements, strategic coordination mechanisms, resource management practices, and patterns of interaction between governmental and non-governmental actors involved in defense innovation. Five predominant public administration approaches identified in international practice have been systematized: strategic and coordination-oriented, institutional and organizational, centralized and institutional, resource-adaptive, and partnership and innovation-oriented. Directions for the selective adaptation of international experience to Ukraine's national circumstances have been substantiated, focusing on improving organizational coordination, procedures for testing and deploying intelligent technologies, human resource development, partnerships, risk management, and technological resilience. It has been established that the application of international public administration practices should take into consideration Ukraine's defense priorities, institutional environment, resource capacities, and security constraints.

The principal challenges of public administration associated with the use of artificial intelligence to enhance Ukraine's defense capabilities have been systematized, and their interconnected nature has been established. A scientific and methodological approach to optimizing the relevant public administration processes has been further developed. This approach encompasses the systematization of administrative problems and mechanisms for addressing them, the establishment of criteria for prioritizing administrative responses, the differentiated selection of optimization instruments, and the assessment of their effectiveness using appropriate performance indicators. A distinctive feature of the proposed approach is the integration of problem-oriented administrative intervention with adaptability, enabling the revision of priorities, mechanisms, and management instruments in response to changes in the security environment, defense requirements, and the actual outcomes of artificial intelligence applications.

It has been substantiated that the implementation of the problem-adaptive approach involves a continuous relationship between identifying administrative problems, establishing priorities for their resolution, selecting appropriate mechanisms, implementing administrative measures, and evaluating the results achieved. Performance evaluation is regarded not merely as the final stage of the administrative process but also as a feedback mechanism that facilitates the timely identification of emerging problems, clarification of their underlying causes, and adjustment of administrative decisions. It has been demonstrated that the application of this approach creates favorable conditions for improving the justification and quality of administrative decisions, reducing organizational fragmentation, ensuring more rational resource utilization, strengthening oversight of intelligent technology implementation, and enhancing the adaptability of the public administration system to evolving national defense requirements.

The findings of the dissertation contribute to the development of theoretical provisions and the improvement of scientific and methodological foundations of public administration concerning the use of artificial intelligence to enhance Ukraine's defense capabilities. The proposed theoretical provisions and practical

recommendations may be applied to improve the legal, regulatory, institutional, and organizational frameworks for implementing artificial intelligence to strengthen national defense capability, promote interagency cooperation, enhance the effectiveness of defense planning, and improve public administration processes in response to a dynamically evolving security environment.

Keywords: state administration, artificial intelligence, national defense capability, public administration, defense, national security, public authorities, threats, state policy, defense systems, strategic decisions, digital technologies, digital transformation, digitalization, security and defense sector.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

1. **Пустовіт Я. Б.,** Гбур З. В. Використання штучного інтелекту в підвищенні обороноздатності України: аспекти публічного управління. *Інвестиції: практика та досвід.* 2023. № 13. С. 103-108. DOI: https://doi.org/10.32702/2306-6814.2023.13.103. *(Пустовіт Я. Б. – досліджено можливості використання технологій штучного інтелекту для підвищення обороноздатності України, визначено перспективні напрями їх застосування в секторі безпеки і оборони. Гбур З. В. – розглянуто особливості публічного управління процесами впровадження технологій штучного інтелекту та організаційно-управлінські аспекти їх використання для забезпечення обороноздатності держави).*

2. **Пустовіт Я. Б.,** Гбур З .В. Аналіз існуючих стратегій у державному управлінні щодо використання штучного інтелекту в обороні. *Успіхи та досягнення в науці.* 2024. № 1(1). С. 172-185. DOI: https://doi.org/10.52058/3041-1254-2024-1(1)-172-185. *(Пустовіт Я. Б. – проаналізовано наявні стратегії використання штучного інтелекту в оборонній сфері, визначено основні напрями його застосування для підвищення ефективності оборонної діяльності та підтримки прийняття стратегічних рішень. Гбур З. В. досліджено організаційно-управлінські, нормативно-правові та етичні аспекти впровадження штучного інтелекту в оборонній сфері).*

3. Пустовіт Я. Б. Державна політика щодо використання технологій штучного інтелекту у сфері оборони України. *Актуальні проблеми інноваційної економіки та права.* 2026. №3. С. 191-195. DOI: https://doi.org/10.36887/2524-0455-2026-3-36.

4. Пустовіт Я. Б. Теоретичні засади використання штучного інтелекту в системі публічного управління обороноздатністю держави. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. Вип. 356(4). С. 189-195.

DOI: https://doi.org/10.31891/2307-5740-2026-356-26.

Тези наукових доповідей

5. Пустовіт Я. Б. Обробка фінансової інформації в умовах війни: програми та технології. *Тренди сталого розвитку для України* : I Науково-практична конференція за міжнародною участю, м. Чернігів – м. Київ, 10 липня 2024 року : тези доповіді. Чернігів : УТМ, 2024. С. 80-84.

6. Пустовіт Я. Б. Аспект публічного управління: використання штучного інтелекту в обороноздатності України. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : I Міжнародна науково-практична конференція, м. Переяслав, 2 червня 2023 року : тези доповіді / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 224-226.

7. Пустовіт Я. Б. Штучний інтелект та публічне управління. *Складові національної безпеки в умовах воєнного стану* : Науково-практична конференція з міжнародною участю, м. Київ, 9-11 серпня 2023 року : тези доповіді / за заг. ред. З. В. Гбур. Кам'янець-Подільський : Друкарня Рута, 2023. С. 102-111.

8. Пустовіт Я. Б. Використання штучного інтелекту в обороноздатності України. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : II Міжнародна науково-практична конференція, м. Переяслав, 27 жовтня 2023 року : тези доповіді / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 192-195.

9. Пустовіт Я. Б. Нормативно-правова база використання штучного інтелекту в обороні. *Стратегічні пріоритети менеджменту і адміністрування у повоєнний період* : V Міжнародна науково-практична інтернет-конференція, м. Харків, 26 квітня 2024 року : тези доповіді. 2024. С. 150-153.

10. Пустовіт Я. Б. Аналіз існуючих стратегій використання штучного інтелекту в обороні. *Національна безпека України в умовах воєнного стану* : I Науково-практична конференція з міжнародною участю, м. Чернігів, 6-8 березня 2024 року : тези доповіді / за заг. ред. З. В. Гбур. Чернігів : ІПТ, 2024. С. 212-216.

11. Пустовіт Я. Б. Цивільно-військове співробітництво в інноваційних розробках: політика щодо штучного інтелекту. *Сучасний стан та пріоритети*

модернізації науки, освіти, технологій та суспільства : Міжнародна науково-практична конференція, м. Ізмаїл, 16 квітня 2025 року : тези доповіді. Ізмаїл : ЦФЕНД, 2025. С. 56-57.

12. Пустовіт Я. Б. Державна політика використання штучного інтелекту в оборонній сфері України. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : VII Міжнародна наукова конференція, м. Харків, 31 липня 2026 року : тези доповіді / Міжнародний центр наукових досліджень. Вінниця : ТОВ «УКРЛОГОС Груп», 2026. С. 56–58.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 19
ВСТУП 21
РОЗДІЛ І. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ОБОРОНОЗДАТНОСТІ ДЕРЖАВИ 33
1.1. Генезис штучного інтелекту та еволюція наукових підходів до визначення його сутності 33
1.2. Обороноздатність держави як об’єкт публічного управління в системі національної безпеки 54
1.3. Теоретичні підходи до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони 81
Висновки до розділу 1 98
Розділ ІІ. ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМУ ПУБЛІЧНОГО УПРАВЛІННЯ ОБОРОНОЗДАТНІСТЮ 102
2.1. Нормативно-правове забезпечення та правове регулювання застосування технологій штучного інтелекту в сфері національної безпеки й оборони. 102
2.2. Суб’єкти публічного управління та їх функціональна взаємодія при впровадженні ШІ у сфері обороноздатності 124
2.3. Інтеграція ШІ-рішень у процеси управлінської діяльності як чинник підвищення обороноздатності України 143
Висновки до розділу 2 164
РОЗДІЛ ІІІ. НАПРЯМИ ВДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ 168
3.1. Зарубіжний досвід публічного управління використання штучного інтелекту для підвищення обороноздатності держави 168
3.2. Проблеми публічного управління використання штучного інтелекту для підвищення обороноздатності України та шляхи їх вирішення 188
Висновки до розділу 3 205

ВИСНОВКИ 207
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 213
ДОДАТКИ 240

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БПЛА	–	безпілотний літальний апарат
ЄС	–	Європейський Союз
ЗСУ	–	Збройні сили України
МОУ	–	Міністерство оборони України
НАТО	–	Організація Північноатлантичного договору (або Північноатлантичний альянс).
НКЕК	–	Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку
ООН	–	Організація об'єднаних націй
РНБО	–	Рада національної безпеки і оборони України
СБУ	–	Служба безпеки України
США	–	Сполучені Штати Америки
ШІ / AI	–	Штучний інтелект / Artificial Intelligence
ЮНЕСКО	–	Організація Об'єднаних Націй з питань освіти, науки і культури (англ. UNESCO – United Nations Educational, Scientific and Cultural Organization)
AI Act / EU AI Act	–	Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту (Акт про штучний інтелект)
EDPS	–	Європейський інспектор з захисту даних
G7	–	Група семи
GDPR	–	General Data Protection Regulation – закон ЄС щодо обробки персональних даних
HRW	–	правозахисна організація Human Rights Watch
IEC	–	Міжнародна електротехнічна комісія
IHRC	–	Міжнародна клініка з прав людини Гарвардської юридичної

школи

ISO	–	Міжнародна організація зі стандартизації
NIST	–	Національний інститут стандартів і технологій США
OECD / OECP	–	Організація економічного співробітництва та розвитку
SIPRI	–	Стокгольмський інститут дослідження проблем миру

ВСТУП

Актуальність теми. В умовах стрімкого розвитку цифрових технологій, трансформації характеру сучасних збройних конфліктів та посилення глобальних безпекових викликів особливого значення набуває використання штучного інтелекту як інноваційного інструменту підвищення обороноздатності держави. Технології штучного інтелекту поступово стають невід'ємною складовою сучасних систем оборонного планування, інформаційно-аналітичного забезпечення, стратегічного прогнозування, управління ресурсами та підтримки прийняття управлінських рішень. Їх упровадження відкриває нові можливості для підвищення оперативності, обґрунтованості та результативності управлінських процесів у секторі безпеки і оборони, водночас зумовлюючи необхідність переосмислення традиційних підходів до організації публічного управління. За таких обставин штучний інтелект слід розглядати не лише як сукупність перспективних технологічних рішень, а й як чинник трансформації механізмів державного управління, що потребує формування належного нормативно-правового, організаційного, інституційного та інформаційно-аналітичного забезпечення.

Особливої актуальності зазначена проблематика набуває для України в умовах повномасштабної збройної агресії Російської Федерації, яка супроводжується інтенсивним застосуванням новітніх технологій, розвитком безпілотних систем, удосконаленням засобів розвідки, автоматизованого оброблення інформації та цифрових систем управління. Необхідність своєчасного реагування на динамічні зміни безпекового середовища, забезпечення ефективної міжвідомчої взаємодії, раціонального використання оборонних ресурсів і підвищення спроможності сил безпеки і оборони України актуалізує питання системного впровадження технологій штучного інтелекту в управлінську діяльність. Водночас практичне використання таких технологій супроводжується низкою проблем, пов'язаних із недостатньою узгодженістю нормативно-правового регулювання, необхідністю вдосконалення інституційної

координації, забезпеченням захисту інформації, технологічної сумісності, підзвітності та відповідальності за прийняття рішень за допомогою систем штучного інтелекту. Виникає об'єктивна потреба в науковому обґрунтуванні напрямів удосконалення механізмів публічного управління використання штучного інтелекту у сфері оборони, розробленні комплексних підходів до його інтеграції в діяльність відповідних державних інституцій та формуванні дієвої моделі управління, орієнтованої на зміцнення обороноздатності, технологічної стійкості й безпекового потенціалу України.

Важливим аспектом актуальності дослідження є необхідність формування цілісної державної політики щодо впровадження та використання технологій штучного інтелекту у сфері забезпечення обороноздатності України. Сучасні тенденції розвитку оборонних технологій засвідчують поступовий перехід від традиційних моделей управління до інтелектуалізованих систем, здатних забезпечувати оброблення значних масивів інформації, виявлення потенційних загроз, прогнозування розвитку безпекових ситуацій та інформаційно-аналітичну підтримку управлінських рішень. Однак ефективність застосування таких технологій залежить не лише від рівня їх технічної досконалості, а й від спроможності органів публічної влади забезпечувати належне стратегічне планування, координацію діяльності суб'єктів сектору безпеки і оборони, узгодженість управлінських рішень та контроль за результатами впровадження інновацій. У цьому контексті особливого значення набуває вдосконалення організаційно-правових, інституційних та інформаційно-аналітичних механізмів публічного управління, спрямованих на створення умов для системного, безпечного й результативного використання штучного інтелекту в інтересах оборони держави.

Водночас актуальність обраної теми зумовлюється необхідністю подолання суперечності між зростаючими можливостями технологій штучного інтелекту щодо підвищення обороноздатності держави та недостатньою сформованістю комплексних науково обґрунтованих підходів до публічного управління процесами їх упровадження і використання. Попри активізацію

наукових досліджень, присвячених технологічним, військовим, правовим та етичним аспектам застосування штучного інтелекту, питання його інтеграції в систему публічного управління оборонною сферою потребують подальшого теоретико-методологічного осмислення. Зокрема, наукового обґрунтування потребує державне регулювання використання штучного інтелекту, розмежування повноважень і відповідальності суб'єктів управління, формування ефективних моделей міжвідомчої взаємодії, визначення критеріїв оцінювання результативності впровадження інтелектуальних технологій, а також забезпечення належного співвідношення технологічної автономності систем і людського контролю за управлінськими рішеннями. Зазначене обумовлює необхідність проведення комплексного наукового дослідження, спрямованого на розвиток теоретичних положень і розроблення практичних рекомендацій.

Теоретичним підґрунтям дисертаційного дослідження стали напрацювання вітчизняних і зарубіжних учених у галузі використання штучного інтелекту в оборонній сфері, у публічному управлінні, а також у сфері державного регулювання цифрової трансформації та інституційного розвитку оборонно-промислового комплексу.

Основою для розгляду питання генезису штучного інтелекту, еволюції наукових підходів до визначення його сутності стали класичні та сучасні роботи насамперед зарубіжних науковців. Так, П. Гейс, Б. Деліпетрев, У. Костич, Дж. Маккарті, М. Мінський, П. Норвіг, С. Рассел, А. Тюрінг, К. Цинаракі та інші заклали основи для вивчення штучного інтелекту, описали його головні особливості, окреслили напрями використання у життєдіяльності суспільства та обґрунтували сутність і шляхи його розвитку. Еволюцію досліджень у галузі штучного інтелекту розглядали П. Гоел, Ю. Двівіді, М. Джаннакіс, В. Дюто, Н. Рана, А. Шарма та інші дослідники. Теоретичною основою розуміння сутності штучного інтелекту стали й напрацювання вітчизняних учених – М. Амосова, О. Баранова, В. Глушкова, О. Івахненка, О. Костенка та інших. Зокрема, наукові здобутки В. Глушкова стали основою для розвитку концепції інтелектуальних інформаційних систем, автоматизованого опрацювання великих масивів даних і

методів розпізнавання образів. Сучасну стратегію розвитку штучного інтелекту в Україні розглядає, зокрема, А. Шевченко.

Питання обороноздатності та сфери безпеки та оборони аналізують у своїх працях С. Бєлай, В. Богданович, П. Богуцький, О. Вольська, Я. Григоренко, В. Дабіжа, Л. Демидова, О. Кузьменко, А. Некряч, В. Пасічко, Л. Перевалова, І. Свида, В. Сироватко, Є. Скулиш, К. Споришев, В. Троцько, М. Цибуленко та багато інших. Наприклад, у праці А. Некряч розкрито теоретичні та правові засади державного управління у сфері застосування штучного інтелекту для захисту інформаційного простору та зміцнення обороноздатності України. Велика кількість науковців зазначають, що у сфері безпеки та оборони, а також для підвищення обороноздатності держави варто використовувати технології штучного інтелекту. Важливою проблемою для наукової спільноти залишається сфера регулювання та управління обороноздатністю, саме тому актуальним напрямком досліджень є впровадження штучного інтелекту в публічне управління з метою посилення обороноздатності. Аналіз штучного інтелекту як інструменту публічного управління здійснюють В. Василенко, О. Вольська, Ю. Даник, А. Дикий, О. та Ю. Карпенки, В. Корсун, К. Споришев, В. Шестаков та багато інших. Ця ж проблематика є предметом дослідження зарубіжних вчених – наприклад, Дж. Буллока, Б. Вірца, Дж. Вайрера, К. Гаєра.

Нагальною проблемою, зокрема для України, залишається правове регулювання застосування штучного інтелекту в різних сферах суспільного життя, і насамперед у секторі забезпечення обороноздатності, що набуває особливої гостроти в умовах триваючої збройної агресії рф. А. Гачкевич, В. Дабіжа, К. Споришев, Т. Федоренко та інші науковці вказують на недосконаліть і фрагментарність сучасного українського законодавства щодо регулювання сфери штучного інтелекту. Їхні праці стали підґрунтям для аналізу та узагальнення нормативно-правового забезпечення зазначеної галузі.

Попри високу цінність і різноплановість наукових праць зазначених авторів, більшість із них висвітлюють лише окремі технологічні, правові або загальноуправлінські аспекти застосування штучного інтелекту зокрема у сфері

обороноздатності. Водночас у вітчизняній науці публічного управління залишається недостатньо розробленою проблема створення цілісної інституційної архітектури та концептуально-методологічного забезпечення впровадження штучного інтелекту в сектор безпеки і оборони України. Необхідність подолання нормативно-правової фрагментарності, оптимізації міжвідомчої координації та забезпечення демократичного контролю над використанням ШІ-технологій в умовах триваючої воєнної агресії зумовлює вибір теми, мети та завдань даного дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження відповідає проблематиці науково-дослідної роботи кафедри міжнародних відносин та політичного консалтингу Інституту права та суспільних відносин ЗВО «Відкритий міжнародний університет розвитку людини «Україна» за темою «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (№ державної реєстрації 0124U000322) (довідка № 12/23-27304.2024 р. від 05.10.2026), у межах якої автором досліджено теоретико-методологічні та організаційно-правові засади використання штучного інтелекту в підвищенні обороноздатності України, зокрема: визначено місце і роль штучного інтелекту в системі публічного управління забезпечення обороноздатності держави; проаналізовано нормативно-правове та інституційне забезпечення впровадження технологій штучного інтелекту в секторі безпеки і оборони України; систематизовано зарубіжний досвід застосування інтелектуальних технологій в оборонній сфері; обґрунтовано напрями вдосконалення механізмів публічного управління використанням штучного інтелекту, спрямованих на підвищення ефективності інформаційно-аналітичного забезпечення, підтримки прийняття управлінських рішень та зміцнення обороноздатності України.

Мета і завдання дослідження. Метою дисертаційного дослідження є теоретико-методологічне обґрунтування засад використання штучного інтелекту в системі публічного управління у сфері оборони, визначення особливостей і проблем його впровадження та розроблення науково-практичних рекомендацій

щодо вдосконалення механізмів публічного управління використання технологій штучного інтелекту для підвищення обороноздатності України.

Для досягнення поставленої мети було визначено і вирішено такі завдання:

- систематизувати основні наукові підходи до визначення сутності штучного інтелекту та уточнити понятійно-категоріальні засади його розуміння в контексті публічного управління;
- розкрити сутність обороноздатності держави як об'єкта публічного управління в системі національної безпеки, обґрунтувати взаємозв'язок між оборонним потенціалом, управлінськими процесами й формуванням оборонних спроможностей;
- систематизувати теоретичні підходи до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони та визначити основні функціональні напрями його застосування в процесах забезпечення обороноздатності держави;
- дослідити нормативно-правову базу використання ШІ для посилення обороноздатності України, проаналізувати переваги та недоліки чинного законодавства, окреслити напрямки його подальшого вдосконалення;
- розглянути цілісну інституційну структуру впровадженні ШІ у сфері обороноздатності, визначити функціональні обов'язки суб'єктів публічного управління та особливості їх взаємодії;
- узагальнити зарубіжний досвід публічного управління використання штучного інтелекту для підвищення обороноздатності держави;
- систематизувати проблеми публічного управління використання штучного інтелекту для підвищення обороноздатності України.

Об'єкт дослідження – процеси публічного управління у сфері забезпечення обороноздатності України.

Предмет дослідження – теоретико-методологічні засади, організаційно-правові та інституційні механізми публічного управління використання штучного інтелекту для підвищення обороноздатності України.

Методи дослідження. Для досягнення поставленої мети та розв'язання

визначених завдань у дисертаційній праці використано комплекс теоретичних підходів, а також загальнонаукових і спеціальних методів наукового пізнання. Зокрема, історичний та діалектичний підходи дали змогу дослідити еволюцію штучного інтелекту та наукових підходів до розуміння його сутності, встановити етапи його розвитку та використання, еволюції та трансформації управлінської парадигми в секторі безпеки і оборони. Застосування компаративного підходу дозволило порівняти нормативно-правове забезпечення використання штучного інтелекту в різних країнах світу. Системний та системно-структурний аналіз слугували основою для розробки цілісної інституційної архітектури використання штучного інтелекту в оборонній сфері України, виокремлення її ключових суб'єктів і встановлення взаємозв'язків між ними. Структурно-функціональний метод використано при визначенні функцій та повноважень державних органів, військового управління, регуляторів та оборонних кластерів у процесі впровадження ШІ-рішень. Для уточнення понять «штучний інтелект», «обороноздатність», «публічне управління» та інших використано методи аналізу та синтезу. Метод узагальнення допоміг зробити висновки про необхідність вдосконалення правового забезпечення означеної сфери, визначити інституційну складову регулювання використання технологій штучного інтелекту в оборонній галузі. При розгляді конкретних прикладів використання штучного інтелекту у публічному управлінні – під час прогнозування, планування, програмування, організації та регулювання, координації та контролю – було використано метод кейс-стаді, який є незамінним для практичного аналізу реального досвіду впровадження конкретних технологічних рішень та інституційних проєктів у секторі безпеки і оборони України під час війни, що дало змогу виявити прикладні проблеми інституціоналізації ШІ-рішень та оцінити їхню ефективність у реальних умовах. Формально-юридичний метод використано під час аналізу вітчизняної та зарубіжної нормативно-правової бази, виявлення прогалин і фрагментарності законодавства щодо регулювання штучного інтелекту, а також обґрунтування пропозицій щодо його вдосконалення. Структурно-логічний метод та метод моделювання допомогли

візуалізації та схематичному побудуванню процесів трансформації парадигми управління. Метод узагальнення та наукової абстракції використано для підсумкового формулювання концептуальних висновків, теоретичних узагальнень і практичних рекомендацій щодо посилення обороноздатності України за допомогою використання ШІ-технологій та використання їх у системі публічного управління.

Застосований комплекс методів забезпечив системність і об'єктивність дослідження, що уможливило виконання визначених завдань та формування здобутих результатів наукової новизни.

Інформаційно-джерельну базу дослідження становлять нормативно-правові акти України, що регулюють сфери національної безпеки, оборони, публічного управління та цифрової трансформації; міжнародно-правові документи, директиви та рекомендації Європейського Союзу, НАТО та інших міжнародних організацій щодо етичних, безпекових і правових аспектів застосування штучного інтелекту; офіційні статистичні, аналітичні та звітні матеріали Міністерства оборони України, Генерального штабу Збройних Сил України, Міністерства цифрової трансформації України та інших суб'єктів публічного управління; емпіричні дані та практичні матеріали щодо функціонування вітчизняних інноваційних оборонних екосистем і цифрових платформ, інформаційні дані з відкритих Інтернет-ресурсів; наукові праці, аналітичні доповіді та монографічні дослідження вітчизняних і зарубіжних учених у галузі публічного управління, правознавства, воєнних наук та штучного інтелекту, а також публікації у провідних наукових періодичних виданнях, матеріали міжнародних і всеукраїнських науково-практичних конференцій та власні аналітичні напрацювання автора дисертаційного дослідження.

Наукова новизна одержаних результатів полягає в комплексному теоретико-методологічному обґрунтуванні засад використання штучного інтелекту в системі публічного управління у сфері забезпечення обороноздатності України, а також у розробленні науково-практичних підходів до вдосконалення механізмів публічного управління процесами впровадження та

використання технологій штучного інтелекту в діяльності суб'єктів сектору безпеки і оборони. За результатами проведеного дослідження сформульовано такі основні положення наукової новизни:

удосконалено:

- теоретичний підхід до розгляду обороноздатності держави як комплексного об'єкта публічного управління в системі національної безпеки шляхом розмежування її структурних складових і чинників впливу та обґрунтування інтегрувальної ролі публічно-управлінського узгодження у процесі перетворення оборонного потенціалу на оборонні спроможності, що передбачає взаємозв'язок стратегічного планування, координації діяльності суб'єктів, ресурсного забезпечення, моніторингу та адаптивного коригування управлінських рішень відповідно до змін безпекового середовища;
- науковий підхід до нормативно-правового забезпечення використання штучного інтелекту у сфері обороноздатності України шляхом систематизації чинних правових і стратегічних засад, виявлення прогалин та суперечностей правового регулювання й обґрунтування напрямів його вдосконалення, що передбачає комплексне врахування особливостей оборонної сфери, міжнародних стандартів, вимог людського контролю, підзвітності та відповідальності за застосування ШІ-систем, що створює передумови для формування узгодженої нормативно-правової основи їх упровадження в систему публічного управління обороноздатністю держави;
- розуміння функціональної взаємодії суб'єктів публічного управління при впровадженні ШІ у сфері обороноздатності держави за допомогою п'яти взаємопов'язаних функціональних блоків, які включають в себе органи публічного управління, практичних споживачів реального бойового застосування та розробників технологій штучного інтелекту та цифрових інновацій;
- науково-методичний підхід до оптимізації публічного управління використання штучного інтелекту для підвищення обороноздатності України, який передбачає комплексне розв'язання проблем на основі взаємозв'язку

механізмів їх оптимізації, критеріїв визначення пріоритетності управлінського реагування, диференційованого добору відповідних механізмів та показників оцінювання результативності, що створює передумови для підвищення обґрунтованості управлінських рішень, узгодженості діяльності суб'єктів сектору безпеки і оборони та адаптивності управлінських процесів до змін оборонних потреб і безпекового середовища.

набули подальшого розвитку:

- теоретико-методологічні засади розуміння сутності штучного інтелекту, конкретизація його характеристик за допомогою систематизації та порівняльного аналізу зарубіжних і вітчизняних наукових підходів, що дозволило розглянути штучний інтелект як інструмент публічного управління, який пройшов шлях від суто технологічного до універсального;
- теоретичні положення щодо використання штучного інтелекту в системі публічного управління сектором безпеки і оборони шляхом систематизації інструментального, аналітико-прогностичного, інституційно-управлінського, ризик-орієнтованого та адаптивного підходів і обґрунтування взаємопов’язаних функціональних напрямів його застосування, зокрема інформаційно-аналітичного, прогностичного, планувально-ресурсного, координаційного та контрольно-моніторингового;
- наукові підходи до систематизації зарубіжного досвіду публічного управління використання штучного інтелекту для підвищення обороноздатності держави за допомогою виокремлення критерію домінантного управлінського пріоритету стратегічно-координаційного, інституційно-організаційного, централізовано-інституційного, ресурсно-адаптивного та партнерсько-інноваційного підходів, що дало змогу обґрунтувати шість взаємопов'язаних напрямів вибіркової адаптації відповідних управлінських механізмів до інституційних, ресурсних і безпекових умов України.

Практичне значення отриманих результатів полягає в розробленні науково-практичних положень і рекомендацій щодо вдосконалення механізмів публічного управління впровадження технологій штучного інтелекту, розвитку

інформаційно-аналітичного забезпечення, оптимізації управлінських процесів та підвищення ефективності прийняття управлінських рішень у сфері забезпечення обороноздатності України. Підтвердженням наукової та практичної цінності отриманих результатів дисертаційного дослідження є:

- результати дисертаційного дослідження впроваджено в освітній процес ЗВО «Відкритий міжнародний університет розвитку людини «Україна» та використано під час розроблення робочих програм, силабусів і викладання навчальних дисциплін «Інформаційні війни» та «Міжнародна та національна безпека» за другим (магістерським) рівнем вищої освіти (довідка про впровадження № 12/23-272 від 05.10.2026 р.);
- науково-практичні положення та рекомендації щодо систематизації функціональних можливостей штучного інтелекту в публічному управлінні, використання інтелектуальних технологій для автоматизованого опрацювання інформації, виявлення взаємозв'язків між даними та інформаційно-аналітичної підтримки управлінських рішень використано в діяльності Управління виявлення та розшуку активів Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, з метою вдосконалення інформаційно-аналітичного забезпечення, розвитку цифрових інструментів аналізу даних та підвищення ефективності управлінських процесів (довідка про впровадження № 02-35/2026 від 21.09.2026 р.).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею, у якій автором обґрунтовано теоретико-методологічні засади використання штучного інтелекту у сфері забезпечення обороноздатності України, визначено особливості його впровадження в систему публічного управління та розроблено науково-практичні рекомендації щодо вдосконалення інструментів публічного управління використання технологій штучного інтелекту в діяльності суб'єктів сектору безпеки і оборони України. Основні наукові положення, висновки та рекомендації сформульовано автором особисто. З наукових публікацій, виданих у співавторстві, у роботі використано лише ті

положення, які становлять особистий внесок автора, про що зазначено в переліку публікацій.

Апробація матеріалів дисертації. Основні науково-теоретичні положення та практичні результати дисертаційного дослідження були оприлюднені на: І Міжнародній науково-практичній конференції «Сучасні аспекти реформування системи публічного управління в умовах воєнного часу» (м. Переяслав, 2 червня 2023 р.); Науково-практичній конференції з міжнародною участю «Складові національної безпеки в умовах воєнного стану» (м. Київ, 9-11 серпня 2023 р.); ІІ Міжнародній науково-практичній конференції «Сучасні аспекти реформування системи публічного управління в умовах воєнного часу» (м. Переяслав, 27 жовтня 2023 р.); І Науково-практичній конференції з міжнародною участю «Національна безпека України в умовах воєнного стану» (м. Чернігів, 6-8 березня 2024 р.); V Міжнародній науково-практичній інтернет-конференції «Стратегічні пріоритети менеджменту і адміністрування у повоєнний період» (м. Харків, 26 квітня 2024 р.); І Науково-практичній конференції за міжнародною участю «Тренди сталого розвитку для України» (м. Чернігів – м. Київ, 10 липня 2024 р.); Міжнародній науково-практичній конференції «Сучасний стан та пріоритети модернізації науки, освіти, технологій та суспільства» (м. Ізмаїл, 16 квітня 2025 р.); VII Міжнародній науковій конференції «Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти» (м. Харків, 31 липня 2026 р.).

Публікації. Основні положення дисертаційного дослідження викладено у 12 наукових працях, з яких 4 статті у наукових фахових виданнях України, 8 тез наукових доповідей.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 247 сторінок. Дисертація містить 15 таблиць, 11 рисунків та 4 додатки. Список використаних джерел містить 228 найменувань.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ОБОРОНОЗДАТНОСТІ ДЕРЖАВИ

1.1. Генезис штучного інтелекту та еволюція наукових підходів до визначення його сутності

Сучасний період державного розвитку вирізняється одночасним ускладненням безпекового контексту, стрімким зростанням обсягів інформації та прискоренням технологічної трансформації. Для системи публічного управління це зумовлює потребу не тільки реагувати на вже існуючі загрози, а й завчасно їх виявляти, визначати потенційні наслідки, моделювати можливі сценарії перебігу подій і забезпечувати належну обґрунтованість управлінських рішень. Особливої уваги зазначені процеси набувають у сфері обороноздатності, де помилкові рішення можуть спричинити стратегічні наслідки для держави, її територіальної цілісності, людського потенціалу та стійкості державних інституцій.

За таких обставин цифрові технології поступово втрачають статус виключно допоміжного засобу державного управління. Вони стають складовою інституційної спроможності держави, визначаючи оперативність опрацювання інформації, ефективність планування ресурсів, можливості прогнозування ризиків, координацію взаємодії органів влади та розвиток нових інструментів контролю. Серед технологій, що найбільш суттєво трансформують підходи до роботи з інформацією та ухвалення рішень, особливе місце належить штучному інтелекту (ШІ). Водночас його сучасний зміст неможливо повною мірою розкрити лише шляхом характеристики окремих цифрових інструментів чи прикладів їх застосування.

Для вивчення використання штучного інтелекту з метою посилення обороноздатності України насамперед потрібно визначити зміст цього поняття, простежити формування уявлень про машинний інтелект, охарактеризувати

наукові підходи до його розуміння, що сформувалися в різні історичні періоди, а також встановити ознаки, які дають змогу відрізнити штучний інтелект від традиційної автоматизації, стандартного програмного забезпечення та інших цифрових технологій. У зв'язку з цим обґрунтованим є послідовне дослідження історико-наукового розвитку поняття «штучний інтелект», його сучасного категоріально-понятійного апарату та специфіки застосування в системі публічного управління.

Розгляд ШІ лише як алгоритмів чи технологічного продукту залишає поза увагою управління даними, відповідальність, людський контроль, правові обмеження, ризики та інституційну спроможність. Натомість розуміння ШІ як соціотехнічного явища поєднує його технологічні можливості з публічним управлінням і показує, як він посилює безпеково-оборонні спроможності держави [228].

Ідея штучного інтелекту виникла ще до сучасних комп'ютерів на перетині філософії, логіки, математики, психології та інженерії. Мислителі різних епох досліджували сутність і формалізацію мислення та зв'язок розуму з механізмами, а тому історія становлення ШІ – це не один винахід, а поступове об'єднання ідей про формальне міркування, обчислення, навчання й автономність.

Важливою теоретико-методологічною передумовою становлення сучасного штучного інтелекту став розвиток математичної логіки. Зокрема, у фундаментальній праці «An Investigation of the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities» (Дослідження законів мислення, на яких ґрунтуються математичні теорії логіки та ймовірностей) ще у 1854 р. Дж. Буль обґрунтував можливість формалізації логічних міркувань за допомогою математичних операцій, заклавши підґрунтя для подальшого розвитку символічної логіки та обчислювальних систем [166]. Упродовж XIX–XX століть зазначені ідеї поступово інтегрувалися з досягненнями математичної статистики, теорії обчислень та розвитком електронно-обчислювальної техніки, створивши науково-технологічні

передумови формування штучного інтелекту як самостійного напряму досліджень. У межах довгострокової дослідницької ініціативи Стенфордського університету «Stanford One Hundred Year Study on Artificial Intelligence, AI100» (Стенфордське столітнє дослідження штучного інтелекту) наголошується, що, хоча штучний інтелект як окрема наукова галузь сформувався в середині 1950-х років, його концептуальні та наукові витоки сягають значно давнішого періоду [216].

Вагомий внесок у формування теоретичних засад штучного інтелекту здійснив британський математик і логік А. Тюрінг, який у науковій статті «Computing Machinery and Intelligence» (Обчислювальні машини та інтелект), опублікованій 1950 р. в журналі «Mind», порушив фундаментальне питання щодо можливості відтворення інтелектуальної поведінки за допомогою обчислювальних машин. Уникаючи необхідності однозначного визначення сутності поняття «мислення», дослідник запропонував розглядати здатність машини демонструвати інтелектуальну поведінку через процедуру «імітаційної гри» (imitation game), яка згодом набула поширення під назвою «тест Тюрінга». Запропонований підхід став важливим етапом у розвитку наукових уявлень про машинний інтелект, оскільки передбачав перенесення дослідницької уваги з філософського осмислення природи мислення на оцінювання зовнішніх проявів інтелектуальної поведінки машини в процесі її взаємодії з людиною [220].

Методологічне значення запропонованого А. Тюрінгом підходу полягало у формуванні передумов для розгляду інтелекту не лише як властивості біологічних систем, а й через сукупність когнітивних функцій, окремі прояви яких можуть бути досліджені, формалізовані та відтворені за допомогою обчислювальних засобів. Постановка питання такого характеру сприяла розвитку наукових уявлень про можливість моделювання інтелектуальної діяльності та заклала концептуальні передумови становлення штучного інтелекту як міждисциплінарної галузі наукових досліджень.

Визначальним етапом інституціоналізації штучного інтелекту як самостійного наукового напряму став у 1956 р. «Дартмутський літній

дослідницький проєкт зі штучного інтелекту» (Dartmouth Summer Research Project on Artificial Intelligence), ініційований Дж. Маккарті, М. Мінським, Н. Рочестером і К. Шенноном. Саме з підготовкою цього проєкту пов'язують запровадження Дж. Маккарті терміна «штучний інтелект» (artificial intelligence), який згодом закріпився в науковому дискурсі [193]. У пропозиції щодо проведення дослідження, підготовленій 1955 р., було сформульовано вихідне припущення про те, що процеси навчання та інші прояви інтелектуальної діяльності принципово можуть бути настільки точно описані, щоб забезпечити можливість їх відтворення машиною [173]. Зазначене положення визначило один із фундаментальних напрямів подальшого розвитку досліджень штучного інтелекту, пов'язаний із формалізацією когнітивних процесів, розробленням алгоритмів машинного навчання та створенням систем, здатних виконувати окремі інтелектуальні функції [193].

Дартмутський літній дослідницький проєкт 1956 р. став важливою передумовою становлення штучного інтелекту як самостійного наукового напряму, сприявши об'єднанню дослідницьких підходів у галузях математичної логіки, теорії обчислень, кібернетики, розпізнавання образів та автоматизації інтелектуальної діяльності. Його значення полягало не лише в утвердженні терміна «штучний інтелект», а й у формуванні спільного дослідницького поля, орієнтованого на розроблення методів і технологій, здатних забезпечувати виконання обчислювальними системами завдань, які традиційно пов'язувалися з інтелектуальною діяльністю людини.

Подальший розвиток теоретико-методологічних засад штучного інтелекту відображено у праці М. Мінського «Steps Toward Artificial Intelligence» (Кроки до штучного інтелекту), опублікованій 1961 р. Дослідник систематизував ключові напрями ранніх досліджень ШІ, серед яких особливе місце посідали евристичний пошук, розпізнавання образів, навчання, планування та індуктивне формування узагальнень [199]. Його дослідження сприяло утвердженню уявлення про інтелектуальну діяльність як складну сукупність взаємопов'язаних функціональних процесів, кожен із яких може бути предметом окремого

наукового дослідження та алгоритмічного відтворення. Унаслідок цього розвиток штучного інтелекту поступово набував прикладного спрямування, пов'язаного з формалізацією окремих когнітивних завдань і розробленням програмних засобів їх розв'язання.

Важливим етапом подальшого становлення штучного інтелекту став розвиток символічного підходу, в основу якого покладено представлення знань за допомогою формалізованих символів, логічних конструкцій і правил опрацювання інформації. Теоретичне обґрунтування цього напряму знайшло відображення у праці Дж. Маккарті та П. Хейса «Some Philosophical Problems from the Standpoint of Artificial Intelligence» (Деякі філософські проблеми з погляду штучного інтелекту), у якій дослідники розглянули проблеми формального представлення знань, логічного міркування та моделювання дій інтелектуальних систем у взаємодії із зовнішнім середовищем [192]. У межах дослідження штучний інтелект розглядався крізь призму здатності обчислювальних систем використовувати формалізовані знання, здійснювати логічні висновки та визначати можливі дії відповідно до заданих цілей, а це вже створило важливі концептуальні передумови для подальшого розвитку систем автоматизованого міркування, представлення знань та інтелектуальної підтримки прийняття рішень.

Подальша еволюція штучного інтелекту характеризувалася нерівномірністю науково-технологічного розвитку, що виявлялася у чергуванні періодів інтенсивізації досліджень, зростання інвестиційної активності та суспільних очікувань із періодами уповільнення технологічного прогресу й скорочення фінансування. У науковій літературі останні набули поширення під назвою «зими ШІ» (AI winters). Їх виникнення було зумовлене насамперед невідповідністю між прогнозованими можливостями інтелектуальних систем і фактичними результатами їх практичного застосування, обмеженістю обчислювальних ресурсів, недостатнім розвитком алгоритмічних методів та складністю використання формалізованих знань в умовах невизначеності [177].

Перший період спаду досліджень штучного інтелекту, який переважно

датують 1974-1980 роками, був пов’язаний із критичним переосмисленням можливостей ранніх інтелектуальних програм, зниженням інституційної підтримки та скороченням фінансування відповідних наукових розробок. Попри здатність таких систем виконувати окремі логічні й обчислювальні завдання, їх функціонування залишалося обмеженим заздалегідь визначеними умовами та недостатньо пристосованим до складних ситуацій реального середовища.

Відновлення інтересу до технологій штучного інтелекту на початку 1980-х років значною мірою пов’язувалося з розвитком експертних систем, які використовували формалізовані бази знань і правила логічного висновування для розв’язання спеціалізованих завдань. Однак висока вартість розроблення та супроводження таких систем, складність оновлення знань, обмежена адаптивність і залежність від експертного формування правил спричинили нове зниження зацікавленості у відповідних технологіях, цей період орієнтовно охоплює 1987–1993 роки, увійшов в історію науки як друга «зима ШІ» [180].

Узагальнення історичних передумов, характерних особливостей і наслідкі в зазначених періодів дає змогу визначити їх значення для подальшої трансфор мації наукових підходів до розроблення інтелектуальних систем (табл. 1.1).

Таблиця 1.1

Періоди становлення та кризового розвитку штучного інтелекту: передумови, обмеження й наслідки

Період	Характеристика розвитку	Основні обмеження та наслідки
1956–1974 рр. – початкове піднесення	Становлення символічного ШІ, розвиток евристичного пошуку, логічних програм	Завищені очікування, обмежені обчислювальні можливості, труднощі масштабування
1974–1980 рр. – перша «зима ШІ»	Скорочення фінансування, критичне переосмислення результатів	Зниження інвестиційної активності, необхідність перегляду методів дослідження
1980–1987 рр. – відновлення розвитку	Поширення експертних систем, комерціалізація окремих розробок	Висока вартість підтримки, залежність від формалізованих експертних знань
1987–1993 рр. – друга «зима ШІ»	Спад комерційного інтересу до експертних систем і спеціалізованого обладнання	Скорочення інвестицій, пошук альтернативних технологічних підходів
Із 1990-х рр. – поступове відновлення	Розвиток статистичного машинного навчання, нейронних мереж, інтелектуальних агентів	Перехід до методів, заснованих на даних, із новими вимогами до їх якості та обчислювальних ресурсів

Джерело: узагальнено автором на основі проведених досліджень

Представлена в табл. 1.1 періодизація засвідчує, що розвиток штучного інтелекту визначався не лише внутрішньою логікою науково-технологічного прогресу, а й сукупністю економічних, організаційних та інституційних чинників. Зокрема, зміна пріоритетів фінансування, рівня державної підтримки, інвестиційної зацікавленості та практичних потреб користувачів безпосередньо впливала на інтенсивність досліджень і напрями технологічних розробок. З позицій публічного управління зазначений історичний досвід підтверджує необхідність формування довгострокових підходів до підтримки інновацій, обґрунтованого оцінювання технологічної зрілості та врахування ризиків, пов’язаних із невідповідністю між очікуваними й фактичними результатами впровадження інтелектуальних систем.

Подолання технологічних обмежень ранніх систем штучного інтелекту поступово супроводжувалося розширенням дослідницьких підходів, орієнтованих на використання статистичних методів, машинного навчання та штучних нейронних мереж. На відміну від традиційних символічних систем, функціонування яких переважно ґрунтувалося на попередньо визначених правилах, методи машинного навчання передбачають виявлення закономірностей на основі опрацювання даних і використання результатів навчання для виконання відповідних завдань. Розширення обсягів доступної інформації, підвищення продуктивності обчислювальних засобів і вдосконалення алгоритмів створили передумови для поширення технологій глибокого навчання та істотного розширення сфер практичного застосування ШІ.

Сучасний етап розвитку штучного інтелекту характеризується співіснуванням і взаємодоповненням різних технологічних напрямів, зокрема машинного навчання, глибоких нейронних мереж, оброблення природної мови, комп’ютерного зору, генеративних моделей, методів представлення знань та автоматизованого міркування [46].

Відповідно, штучний інтелект недоцільно ототожнювати виключно з робототехнікою, автономними технічними засобами або експертними

системами, оскільки його функціональні можливості охоплюють прогнозування, класифікацію, розпізнавання, генерацію інформаційного контенту, оптимізацію процесів і підтримку прийняття рішень.

Різноманітність технологічних підходів та функціональних можливостей штучного інтелекту зумовила формування відмінних наукових поглядів на визначення його сутності. Упродовж історичного розвитку дослідники розглядали ШІ крізь призму відтворення людської інтелектуальної поведінки, формалізації процесів мислення, алгоритмічного розв'язання складних завдань, навчання на основі даних і раціонального вибору дій. Відтак сучасне розуміння штучного інтелекту має міждисциплінарний характер та охоплює технічний, когнітивний, функціональний, правовий і управлінський виміри.

Одну з найбільш поширених систематизацій наукових підходів до розуміння штучного інтелекту запропонували С. Рассел і П. Норвіг у праці «Artificial Intelligence: A Modern Approach» (Штучний інтелект: сучасний підхід). Дослідники виокремили чотири концептуальні напрями, у межах яких інтелектуальні системи розглядаються з позицій здатності мислити подібно до людини, діяти подібно до людини, мислити раціонально або діяти раціонально. Запропонована дослідниками класифікація дозволяє розмежувати підходи, орієнтовані на відтворення людських когнітивних процесів і поведінки, та підходи, у яких визначальним критерієм виступає раціональність міркувань або результативність дій [213].

Для дослідження можливостей використання штучного інтелекту в системі публічного управління особливого значення набуває раціонально-агентний підхід, відповідно до якого інтелектуальна система розглядається як агент, здатний сприймати інформацію про зовнішнє середовище, опрацьовувати її та визначати дії, спрямовані на досягнення поставлених цілей. Застосування зазначеного підходу дозволяє досліджувати штучний інтелект не лише як сукупність алгоритмів, а й як функціональний інструмент інформаційно-аналітичного забезпечення управлінської діяльності.

Розширення функціональних можливостей штучного інтелекту та його

проникнення у сфери суспільної діяльності, що мають стратегічне значення, зумовили необхідність переосмислення підходів до оцінювання ефективності, надійності й безпечності інтелектуальних систем. Якщо на початкових етапах розвитку ШІ наукова увага переважно зосереджувалася на можливості відтворення окремих когнітивних функцій людини, то сучасний етап характеризується посиленням значення питань управління технологічними ризиками, забезпечення прозорості алгоритмічних процесів, дотримання прав людини та визначення відповідальності суб'єктів, залучених до розроблення й використання відповідних технологій [121].

Показовим у цьому контексті є підхід Національного інституту стандартів і технологій США (National Institute of Standards and Technology, NIST), відображений у документі «Artificial Intelligence Risk Management Framework» (AI RMF 1.0). Запропонована концепція передбачає управління ризиками протягом життєвого циклу систем штучного інтелекту та визначає характеристики їхньої надійності, серед яких достовірність і надійність результатів, безпечність, захищеність і стійкість, підзвітність і прозорість, пояснюваність та інтерпретованість, захист приватності, а також справедливість із належним управлінням ризиками шкідливої упередженості [218]. Важливість зазначеного підходу полягає у переході від оцінювання виключно технологічних характеристик ШІ до комплексного врахування організаційних, соціальних та управлінських наслідків його застосування [203].

Подібну спрямованість має Рекомендація ЮНЕСКО з етики штучного інтелекту «Recommendation on the Ethics of Artificial Intelligence», ухвалена в 2021 р. У документі штучний інтелект розглядається з урахуванням динамічного характеру його технологічного розвитку, а особлива увага приділяється системам, здатним виконувати завдання, пов'язані з навчанням, міркуванням, сприйняттям, прогнозуванням, плануванням і контролем. Водночас принципове значення надається забезпеченню людського нагляду, прозорості, відповідальності, недискримінації та дотриманню прав людини [223]. Для сфери публічного управління такий підхід є важливим, оскільки дозволяє розглядати

впровадження штучного інтелекту в нерозривному зв'язку з інституційними механізмами забезпечення законності й суспільної відповідальності.

Подальшу конкретизацію функціонального розуміння штучного інтелекту здійснено в межах Організації економічного співробітництва та розвитку (OECD). У листопаді 2023 року держави – члени OECD погодили оновлене визначення системи ШІ, яке отримало додаткове роз'яснення у відповідному документі 2024 р., де система штучного інтелекту характеризується здатністю на основі отриманих вхідних даних визначати способи формування результатів у вигляді прогнозів, контенту, рекомендацій або рішень, що можуть впливати на фізичне чи віртуальне середовище [205]. Особливого значення набуває визнання різного рівня автономності таких систем та можливості їх адаптації після впровадження, що потребує відповідного врахування в процесі організації управління їх використанням.

Важливим етапом формування правових засад регулювання штучного інтелекту стало прийняття Європейським Союзом Регламенту (ЄС) 2024/1689 (Artificial Intelligence Act, AI Act), яким закріплено нормативне визначення системи штучного інтелекту та запроваджено диференційований підхід до її регулювання залежно від характеру й рівня ризиків, пов'язаних із застосуванням відповідних технологій [210]. Водночас необхідно враховувати, що відповідно до статті 2 зазначеного Регламенту його положення не поширюються на системи штучного інтелекту в тій частині, у якій вони призначені або використовуються виключно для військових, оборонних цілей чи цілей національної безпеки, з урахуванням передбачених Регламентом умов і винятків.

Отже, у контексті дослідження використання штучного інтелекту для підвищення обороноздатності України AI Act становить насамперед методологічний та порівняльно-правовий інтерес, тоді як особливості нормативно-правового забезпечення застосування відповідних технологій в оборонній сфері потребують окремого комплексного аналізу національних і міжнародно-правових актів, який буде здійснено в другому розділі дисертаційного дослідження.

Розвиток штучного інтелекту в Україні має власні історичні та науково-технологічні передумови, пов’язані зі становленням вітчизняної кібернетичної школи, розвитком математичних методів опрацювання інформації, теорії алгоритмів, обчислювальної техніки та дослідженнями моделювання інтелектуальної діяльності людини. Важливо зазначити, що формування відповідних наукових напрямів відбувалося ще в період перебування України у складі СРСР, однак саме діяльність наукових установ, дослідницьких колективів та окремих учених, які працювали на території України, створила підґрунтя для подальшого розвитку національного наукового потенціалу у сфері штучного інтелекту.

Визначальну роль у формуванні зазначених передумов відіграла діяльність В. Глушкова – видатного математика, кібернетика, засновника української наукової школи кібернетики, дослідження якого охоплювали теорію цифрових автоматів, автоматизацію обчислювальних процесів, математичне забезпечення електронно-обчислювальних машин та проблематику штучного інтелекту [24]. Наукові здобутки В. Глушкова сприяли формуванню теоретико-методологічної основи для створення інтелектуальних інформаційних систем, розвитку методів автоматизованого опрацювання даних і розпізнавання образів. Особливе значення мали його дослідження у сфері автоматизації управління, що передбачали використання обчислювальної техніки для інформаційного забезпечення складних організаційних та економічних процесів [24].

Одним із найбільш масштабних напрямів наукової діяльності В. Глушкова стало обґрунтування концепції Загальнодержавної автоматизованої системи збору й оброблення інформації для обліку, планування та управління народним господарством. Попри те, що зазначена концепція не була реалізована в повному обсязі, її розроблення засвідчило прагнення до інтеграції інформаційних ресурсів, обчислювальних потужностей та управлінських процесів у межах єдиної організаційно-технологічної системи. Водночас такі розробки необхідно розглядати насамперед як історичні передумови інформатизації та автоматизації управління, а не як безпосередній аналог сучасних систем штучного інтелекту.

З позицій публічного управління наукова спадщина В. Глушкова становить особливий інтерес, оскільки демонструє раннє усвідомлення значення інформаційно-аналітичного забезпечення, систематизації даних та автоматизації окремих управлінських функцій для підвищення результативності складних організаційних систем. Зазначені ідеї набувають нового змісту в умовах розвитку сучасних технологій штучного інтелекту, здатних не лише опрацьовувати значні обсяги інформації, а й виявляти закономірності, формувати прогнози та забезпечувати аналітичну підтримку прийняття управлінських рішень.

Вагомий внесок у розвиток українських досліджень штучного інтелекту здійснив М. Амосов, наукова діяльність якого охоплювала не лише медицину, а й кібернетику, моделювання мислення, психічних процесів та складних систем. Особливе місце серед його наукових праць посідають «Моделювання мислення і психіки» (1965 р.), «Штучний розум» (1969 р.) та «Алгоритми розуму» (1979 р.), у яких розглядалися проблеми відтворення окремих механізмів інтелектуальної діяльності, функціонування складних систем і можливості використання формалізованих моделей для дослідження процесів мислення [4].

Наукове значення досліджень М. Амосова полягає в розвитку міждисциплінарного підходу до вивчення інтелекту, заснованого на поєднанні положень кібернетики, біології, психології та математичного моделювання. На відміну від підходів, орієнтованих переважно на виконання формалізованих логічних операцій, дослідження вченого були спрямовані на осмислення складної організації інтелектуальної діяльності, взаємозв’язків між окремими функціональними процесами та можливостей їх відтворення у штучних системах, що сприяло розширенню наукових уявлень про природу інтелекту та формуванню теоретичних передумов для подальшого розвитку інтелектуальних систем [4].

Окремий напрям вітчизняних досліджень, пов’язаний із формуванням математичних засад машинного навчання та прогнозування, представлений науковою діяльністю О. Івахненка, який у 1968 році започаткував розвиток методу групового урахування аргументів, заснованого на принципах

індуктивного моделювання та самоорганізації моделей складних процесів. Зазначений метод передбачав побудову математичних залежностей на основі експериментальних даних, добір структури моделей і визначення їх придатності для прогнозування досліджуваних процесів [36].

Значення наукових здобутків О. Івахненка для розвитку штучного інтелекту полягає у формуванні підходів до автоматизованої побудови моделей на основі даних, що є одним із фундаментальних напрямів машинного навчання. У контексті сучасного розвитку інтелектуальних технологій такі дослідження демонструють поступовий перехід від використання виключно заздалегідь визначених правил до застосування методів, здатних виявляти закономірності у складних інформаційних масивах [36]. Для публічного управління відповідні наукові підходи становлять інтерес з огляду на можливості прогнозування, оцінювання альтернативних сценаріїв та інформаційно-аналітичного забезпечення прийняття управлінських рішень.

Новий етап розвитку досліджень штучного інтелекту в Україні пов’язаний із формуванням спеціалізованих наукових установ, розширенням дослідницької інфраструктури та поступовим утвердженням штучного інтелекту як самостійного напряму науково-технологічної діяльності. Важливою подією стало створення 9 жовтня 1991 р. Інституту проблем штучного інтелекту на базі спеціального конструкторського бюро «Інтелект» Донецького державного університету. Його діяльність була спрямована на концентрацію наукового потенціалу у сфері розроблення інтелектуальних систем, інформаційних технологій, робототехніки та дослідження методів штучного інтелекту [37].

Інституційне становлення відповідного наукового напряму супроводжувалося формуванням спеціалізованого науково-інформаційного середовища. Зокрема, у 1995 р. було започатковано науковий журнал «Штучний інтелект», присвячений висвітленню теоретичних і прикладних проблем розроблення інтелектуальних систем. Розвиток таких наукових інституцій і фахових видань створював організаційні передумови для систематизації результатів досліджень, поширення наукових знань та формування професійного

середовища у відповідній галузі.

Подальший розвиток штучного інтелекту в Україні характеризувався розширенням його прикладного використання у сфері інформаційних технологій, автоматизованого аналізу даних, комп'ютерного зору, оброблення природної мови, прогнозування та підтримки прийняття рішень. Водночас зростання практичного значення відповідних технологій поступово зумовило необхідність формування державної політики, спрямованої на підтримку їх розвитку, визначення пріоритетних сфер застосування та створення належних організаційно-правових умов використання [38].

Особливе місце в розвитку сучасних наукових уявлень про сутність штучного інтелекту посідають дослідження українських учених, у яких відповідне поняття розглядається крізь призму технологічних, когнітивних, функціональних, правових та соціальних характеристик. На відміну від ранніх концепцій, зосереджених переважно на можливості відтворення інтелектуальної поведінки людини, сучасні вітчизняні наукові підходи дедалі більше орієнтуються на визначення функціональних можливостей інтелектуальних систем, особливостей їх застосування в суспільних відносинах та необхідності формування належних механізмів правового й управлінського регулювання.

Вагомий внесок у дослідження понятійно-категоріальних засад штучного інтелекту здійснив О. Баранов, який у праці «Визначення терміну «штучний інтелект» обґрунтував необхідність використання міждисциплінарного підходу до формування універсальної дефініції зазначеного поняття. Науковець розглядає штучний інтелект як сукупність методів, способів, засобів і технологій, насамперед комп'ютерних, здатних моделювати когнітивні функції, характеристики яких є еквівалентними відповідним характеристикам когнітивних функцій людини. Принципове значення запропонованого підходу полягає в акцентуванні уваги на функціональній подібності штучного та природного інтелекту без необхідності відтворення біологічних механізмів людського мозку. Водночас дослідник наголошує на важливості технологічної нейтральності визначення, що дозволяє враховувати подальший розвиток

інтелектуальних систем незалежно від конкретних способів їх технічної реалізації [6].

Розвиток правового підходу до визначення штучного інтелекту представлено в дослідженні А. Гачкевича «До питання правової визначеності поняття штучного інтелекту». Автор розглядає штучний інтелект як вид технологій, функціонування яких ґрунтується на застосуванні моделей, сформованих у результаті опрацювання інформації, для створення прогнозів, рекомендацій, рішень та інформаційного контенту. Особливу увагу дослідник приділяє виокремленню характерних ознак ШІ, серед яких інтерактивність, цілеспрямованість, адаптивність, автономність, результативність і системність. Зазначений підхід має важливе значення для формування правових засад використання інтелектуальних систем, оскільки дозволяє конкретизувати їх функціональні характеристики та визначити ознаки, які можуть враховуватися в процесі нормативно-правового регулювання [23].

Інший концептуальний підхід представлений у дослідженні О. Костенка «Штучний інтелект: погляд крізь оптику соціального натуралізму», у якому штучний інтелект розглядається насамперед як цифровий інструмент людської діяльності. Науковець обґрунтовує положення про інструментальну природу ШІ, наголошуючи на тому, що його функціонування та суспільні наслідки використання залежать від діяльності людини й рівня розвитку соціальної культури. Вищевказане є важливим підгрунтям для публічного управління, оскільки дозволяє розмежувати технологічні можливості інтелектуальних систем і владно-управлінські повноваження людини, а також підкреслює необхідність збереження відповідальності уповноважених суб’єктів за прийняті рішення [43].

Для дослідження публічно-управлінського виміру штучного інтелекту важливим є також науковий доробок А. Шевченка, у працях якого проблематика розвитку ШІ розглядається в контексті формування стратегічних пріоритетів держави, розвитку науково-технологічного потенціалу, інституційного забезпечення та визначення шляхів практичного впровадження відповідних

технологій. Саме такі напрямки досліджень розширюють межі суто технологічного розуміння штучного інтелекту та створюють передумови для його аналізу як об’єкта державної політики й інструменту реалізації суспільно значущих завдань [153].

Важливим етапом інституційного оформлення державної політики у зазначеній сфері стало схвалення розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р Концепції розвитку штучного інтелекту в Україні, де визначено основні напрями, пріоритети та завдання розвитку технологій штучного інтелекту, зокрема у сферах освіти, науки, економіки, кібербезпеки, інформаційної безпеки, оборони та державного управління. Прийняття Концепції засвідчило перехід від переважно науково-технологічного осмислення штучного інтелекту до його розгляду як стратегічно важливого напряму державної політики, що потребує узгодженого нормативно-правового, організаційного та ресурсного забезпечення.

Сучасний етап розвитку штучного інтелекту в Україні характеризується посиленням його стратегічного значення для цифрової трансформації держави, модернізації публічного управління, розвитку інноваційної економіки та зміцнення національної безпеки й обороноздатності. Особливої актуальності зазначені процеси набули в умовах повномасштабної збройної агресії Російської Федерації проти України, що зумовило необхідність прискореного впровадження технологічних рішень для аналізу інформації, оцінювання загроз, забезпечення ситуаційної обізнаності та підвищення ефективності управлінських процесів [53].

Важливим напрямом реалізації державної інноваційної політики стало формування Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року, у межах якої штучний інтелект визначено одним із пріоритетних технологічних напрямів, що передбачає розвиток національного інноваційного потенціалу, стимулювання досліджень, створення умов для впровадження сучасних технологій та посилення взаємодії між державою, науковими установами й технологічним сектором [53].

Подальшим кроком у розвитку відповідної інституційної інфраструктури стало започаткування у 2025 р. AI Center of Excellence – центру передового досвіду з розроблення та інтеграції технологій штучного інтелекту при Міністерстві цифрової трансформації України [53]. Серед визначених напрямів його діяльності – створення інтелектуальних рішень для державного сектору, інтеграція ШІ в оборонну сферу, розвиток національних технологічних спроможностей та підтримка досліджень. Зазначені ініціативи відображають поступове розширення ролі держави: від підтримки наукових розробок до формування організаційних умов для практичного впровадження штучного інтелекту в суспільно значущі сфери.

Отже, історичний розвиток штучного інтелекту в Україні характеризується поступовим переходом від фундаментальних досліджень у галузях кібернетики, математичного моделювання та автоматизації інтелектуальної діяльності до формування спеціалізованої наукової інфраструктури й становлення державної політики розвитку та впровадження відповідних технологій. При цьому наукова спадщина українських дослідників створила важливі теоретико-методологічні передумови сучасного розвитку ШІ, тоді як інституційні та нормативно-правові ініціативи останніх років засвідчують його перетворення на інструмент реалізації стратегічних пріоритетів держави.

Узагальнення наукових досліджень зарубіжних та українських учених, а також положень міжнародних рекомендаційних документів і нормативно-правових актів засвідчує відсутність єдиного універсального підходу до визначення сутності штучного інтелекту. Зазначене зумовлено міждисциплінарним характером відповідної категорії, динамічністю розвитку інтелектуальних технологій та відмінностями у визначенні їх функціонального призначення. Водночас простежується поступова трансформація наукових уявлень про штучний інтелект: від акцентування уваги на відтворенні когнітивних функцій і поведінки людини до розгляду інтелектуальних систем як технологічних засобів, здатних опрацьовувати інформацію, формувати прогнози, рекомендації та рішення, функціонувати з різним ступенем

автономності й впливати на суспільні та управлінські процеси. З метою виявлення спільних і відмінних характеристик зазначених підходів, визначення їх концептуальної спрямованості та значення для публічного управління здійснено порівняльну систематизацію, результати якої представлено в табл. 1.2.

Таблиця 1.2.

Еволюція наукових та інституційно-правових підходів до розуміння сутності штучного інтелекту: зарубіжний і вітчизняний досвід

Автор / інституція	Зміст визначення або підходу	Концептуальна спрямованість	Значення для публічного управління
А. Тюрінг (1950 р.)	Оцінювання інтелектуальних можливостей машини через її поведінку в імітаційній грі.	Поведінковий.	Критерії оцінювання результатів роботи інтелектуальних систем.
Дж. Маккарті (1955–2007 рр.)	ШІ як наука та інженерія створення інтелектуальних машин.	Функціонально-технологічний.	Розроблення засобів автоматизації інтелектуальних завдань.
М. Мінський (1961 р.)	Дослідження пошуку, навчання, планування, розпізнавання та інших функцій ШІ.	Функціональний.	Автоматизація окремих інформаційно-аналітичних функцій.
С. Рассел, П. Норвіг (2021 р.)	Систематизація підходів до ШІ за людським і раціональним мисленням та діями.	Когнітивний, раціонально-агентний.	Інформаційна підтримка вибору управлінських дій.
О. Баранов (2023 р.)	ШІ через моделювання когнітивних функцій і використання комп’ютерних технологій.	Міждисциплінарний, когнітивно-функціональний.	Понятійна основа правового регулювання інтелектуальних технологій.
А. Гачкевич (2025 р.)	Технології, що використовують моделі для формування рішень, прогнозів, рекомендацій і контенту.	Функціонально-правовий.	Правова визначеність характеристик і результатів застосування ШІ.
М. Дубняк (2025 р.)	Інтеграція технічних, когнітивних і соціально-правових характеристик ШІ	Інтегративний.	Узгодження технологічних можливостей із правовими вимогами

Продовження таблиці 1.2.

Автор / інституція	Зміст визначення або підходу	Концептуальна спрямованість	Значення для публічного управління
О. Костенко (2026 р.)	ШІ як цифрове знаряддя праці, що залишається інструментом людської діяльності.	Інструментальний, соціально-правовий.	Збереження людської відповідальності та владних повноважень.
Кабінет Міністрів України (2020 р.)	Організована сукупність інформаційних технологій для виконання складних завдань.	Технологічно-функціональний.	Формування державної політики розвитку та застосування ШІ.
UNESCO (2021 р.)	Системи, пов'язані з виконанням когнітивних завдань, із наголосом на етичних вимогах.	Етико-орієнтований.	Людський нагляд, недискримінація, відповідальність.
NIST (2023 р.)	Управління ризиками ШІ з урахуванням надійності, безпечності, прозорості та підзвітності.	Ризик-орієнтований.	Організація оцінювання та управління ризиками.
OECD (2023–2024 р.)	Системи, що формують прогнози, контент, рекомендації або рішення на основі вхідних даних.	Функціонально-агентний.	Оцінювання автономності, результатів і впливу систем.
Європейський Союз (2024 р.)	Нормативне визначення системи ШІ та диференційоване регулювання ризиків.	Нормативно-правовий.	Правові вимоги до розроблення, впровадження та використання систем.

Джерело: узагальнено автором на основі власних досліджень

Результати порівняльного аналізу, представлені в табл. 1.2, дозволяють виокремити декілька взаємопов'язаних напрямів концептуалізації штучного інтелекту. Перший ґрунтується на когнітивно-функціональному розумінні ШІ, у межах якого визначальними є здатність інтелектуальних систем відтворювати окремі функції людського мислення, здійснювати логічні операції та розв'язувати складні завдання. Другий пов'язаний із технологічним і раціонально-агентним підходами, що акцентують увагу на опрацюванні інформації, навчанні, прогнозуванні, формуванні рекомендацій і виборі дій відповідно до поставлених цілей. Третій охоплює нормативно-правові, етичні та ризик-орієнтовані підходи, у яких штучний інтелект розглядається не лише через

його функціональні можливості, а й з урахуванням наслідків застосування, необхідності забезпечення прозорості, підзвітності, безпечності та людського контролю. При цьому дослідження українських учених засвідчують поступове посилення уваги до правової визначеності штучного інтелекту, його інструментальної природи та місця в системі суспільних відносин. З позицій публічного управління зазначене дозволяє розглядати ШІ одночасно як об'єкт регуляторного впливу та інструмент інформаційно-аналітичного забезпечення управлінської діяльності. Водночас специфіка використання відповідних технологій у сфері обороноздатності України потребує подальшого уточнення їх функціонального призначення, меж автономності, механізмів контролю та відповідальності уповноважених суб'єктів.

Проведений порівняльний аналіз наукових та інституційно-правових підходів до визначення сутності штучного інтелекту зумовлює необхідність уточнення його співвідношення із суміжними категоріями, зокрема такими, як «дані», «алгоритм», «модель», «система штучного інтелекту», «машинне навчання», «автоматизація» та «автономність». Зазначені поняття перебувають у тісному взаємозв'язку, проте не є тотожними, оскільки характеризують різні складові, властивості та способи функціонування сучасних інформаційних технологій.

Інформаційну основу функціонування багатьох систем штучного інтелекту становлять дані, які забезпечують можливість навчання моделей ШІ, аналізу закономірностей та формування результатів. Алгоритм визначає формалізовану послідовність операцій для розв'язання певного завдання, тоді як модель відображає встановлені на основі даних або знань залежності, структури чи закономірності, що використовуються для класифікації, прогнозування, генерування результатів та виконання інших функцій. Машинне навчання, своєю чергою, є одним із напрямів розвитку штучного інтелекту, який передбачає формування або вдосконалення моделей на основі даних без необхідності безпосереднього програмування кожного можливого результату.

Принципове значення має розмежування штучного інтелекту та

автоматизації. Остання передбачає виконання визначених операцій із мінімальним або відсутнім безпосереднім втручанням людини, однак сама собою не свідчить про наявність інтелектуальних властивостей системи. На відміну від традиційних автоматизованих засобів, що функціонують переважно відповідно до заздалегідь установлених правил, системи штучного інтелекту здатні на основі отриманих вхідних даних формувати прогнози, рекомендації, рішення або інші результати шляхом використання відповідних моделей і методів обчислювального висновування.

Водночас автономність, що характеризує ступінь самостійності функціонування системи без безпосереднього втручання людини, не може розглядатися як універсальний або самодостатній критерій наявності штучного інтелекту. Інтелектуальні системи можуть функціонувати з різним рівнем автономності, а їх результати – використовуватися як для автоматизованого виконання окремих завдань, так і для інформаційно-аналітичної підтримки прийняття рішень людиною [214]. Отже, сутність штучного інтелекту доцільно визначати не через окрему технологічну характеристику, а через сукупність його функціональних можливостей, особливостей формування результатів і характеру взаємодії з користувачем та середовищем.

Узагальнення результатів дослідження історичної еволюції штучного інтелекту, наукових підходів зарубіжних та українських учених, а також сучасних інституційно-правових трактувань дозволяє констатувати, що сутність зазначеного поняття не може бути вичерпно розкрита виключно через здатність імітувати людське мислення, виконувати обчислювальні операції або автоматизувати окремі процеси. Визначальними характеристиками сучасного штучного інтелекту виступають його здатність до обчислювального опрацювання інформації, виявлення закономірностей, формування висновків і результатів відповідно до визначених цілей, а також можливість функціонування з різним ступенем автономності. При цьому відповідні технологічні можливості набувають практичного значення в межах конкретної діяльності, організаційних процесів та суспільних відносин.

На основі узагальнення результатів дослідження історичної еволюції штучного інтелекту, систематизації наукових підходів зарубіжних та українських учених, а також аналізу сучасних інституційно-правових трактувань набуло подальшого розвитку теоретичне розуміння сутності штучного інтелекту шляхом уточнення його технологічних, функціональних і системних характеристик. З огляду на зазначене, у межах дослідження штучний інтелект пропонується розуміти як сукупність технологій, методів і заснованих на них комп'ютерних систем, здатних на основі опрацювання даних та/або формалізованих знань здійснювати обчислювальне висновування, виявляти закономірності, формувати прогнози, рекомендації, рішення, контент чи інші результати відповідно до визначених цілей, функціонуючи з різним ступенем автономності та забезпечуючи можливість інформаційно-аналітичної підтримки або виконання завдань у різних сферах суспільної діяльності.

Уточнене розуміння штучного інтелекту ґрунтується на поєднанні технологічного, функціонального та системного підходів і передбачає врахування не лише особливостей побудови інтелектуальних систем, а й характеру їх функціонування, способів формування результатів та можливостей використання в організаційних і управлінських процесах. У ході роботи ми прийшли до розуміння, що саме дозволяє розглядати штучний інтелект як технологічний інструмент інформаційно-аналітичного забезпечення, прогнозування та підтримки прийняття рішень, не ототожнюючи автономність його функціонування з наділенням системи владними повноваженнями або самостійною юридичною відповідальністю.

1.2. Обороноздатність держави як об'єкт публічного управління в системі національної безпеки

Обороноздатність держави належить до фундаментальних категорій у системі забезпечення національної безпеки, оскільки характеризує здатність держави захищати власний суверенітет, територіальну цілісність і незалежність

від загроз воєнного характеру. В умовах трансформації сучасного безпекового середовища, зростання інтенсивності збройних конфліктів, поширення гібридних загроз та прискореного розвитку новітніх технологій зміст цієї категорії набуває особливого значення. Обороноздатність дедалі складніше характеризувати виключно через кількісні параметри збройних сил, наявність озброєння, військової техніки чи обсяги матеріальних ресурсів. Її забезпечення передбачає узгоджене функціонування військової, економічної, технологічної, інформаційної, соціальної та організаційно-управлінської складових, які у своїй сукупності визначають спроможність держави протидіяти воєнним загрозам, підтримувати стійкість основних інституцій та адаптуватися до змін безпекового середовища [12].

Особливої актуальності дослідження обороноздатності набуває для України, яка в умовах тривалої збройної агресії Російської Федерації змушена одночасно забезпечувати виконання завдань оборони, мобілізацію наявних ресурсів, функціонування національної економіки, підтримання критичної інфраструктури та розвиток оборонних спроможностей. Повномасштабне вторгнення Російської Федерації у 2022 році засвідчило необхідність комплексного розуміння обороноздатності, за якого результативність збройного захисту держави визначається не лише бойовим потенціалом сил оборони, а й ефективністю державної політики, якістю стратегічного планування, оперативністю прийняття управлінських рішень, спроможністю державних інституцій координувати діяльність різних суб’єктів та забезпечувати раціональне використання обмежених ресурсів [57].

З огляду на зазначене, обороноздатність доцільно досліджувати як комплексну характеристику держави, що формується внаслідок взаємодії наявного оборонного потенціалу, організаційних можливостей його реалізації та результативності управлінських процесів, де можна перейти від переважно військового розуміння обороноздатності до її осмислення як об’єкта публічного управління, забезпечення якого потребує цілеспрямованого впливу держави на процеси формування, розвитку, мобілізації та використання оборонних

ресурсів [137].

Теоретичне дослідження зазначеної категорії потребує насамперед уточнення її змісту та співвідношення із суміжними поняттями, зокрема «оборона», «оборонний потенціал», «оборонні спроможності» та «забезпечення обороноздатності». Незважаючи на змістову спорідненість, наведені категорії характеризують різні сторони функціонування оборонної системи держави, а їх ототожнення ускладнює визначення предмета та меж публічно-управлінського впливу [137].

Вихідним для такого аналізу є законодавче розуміння обороноздатності держави. Відповідно до Закону України «Про оборону України», обороноздатність держави характеризує її здатність до захисту в разі збройної агресії або збройного конфлікту та охоплює сукупність воєнного, економічного, соціального й морально-політичного потенціалу держави, а також відповідних умов його реалізації [97]. Наведений нормативний підхід має принципове значення, оскільки вже на законодавчому рівні визначає обороноздатність як характеристику держави загалом, а не виключно її збройних сил.

Водночас поняття «оборона України» відображає передусім систему заходів, спрямованих на підготовку до збройного захисту держави та здійснення такого захисту, якщо оборона характеризує відповідну діяльність держави, то обороноздатність відображає її здатність забезпечувати виконання оборонних завдань за наявних і прогнозованих умов. Таке розмежування має важливе методологічне значення, оскільки дозволяє визначити обороноздатність як результат взаємодії різних складових державного потенціалу, а забезпечення обороноздатності – як цілеспрямований процес формування необхідних передумов для досягнення такого результату.

Із системних позицій важливе місце посідає категорія «оборонний потенціал», яка характеризує сукупність ресурсів, можливостей і передумов, що можуть бути використані державою для виконання оборонних завдань. До його складу належать військові, економічні, фінансові, матеріально-технічні, кадрові, науково-технологічні, інформаційні та інші ресурси. Проте сама наявність

відповідного потенціалу не гарантує належного рівня обороноздатності, оскільки визначальне значення має здатність держави своєчасно мобілізувати, розподіляти та використовувати наявні ресурси відповідно до характеру загроз і стратегічних пріоритетів оборонної політики [137].

У цьому контексті необхідно розмежовувати оборонний потенціал та оборонні спроможності. Якщо оборонний потенціал характеризує ресурсні й організаційні передумови забезпечення оборони, то оборонні спроможності відображають здатність відповідних суб'єктів, сил і засобів виконувати визначені завдання за встановлених умов. Відтак формування оборонних спроможностей передбачає не лише наявність ресурсів, а й їх належне організаційне поєднання, підготовку персоналу, забезпечення управління, логістики, інформаційного супроводу та взаємодії між відповідними структурами.

З позицій публічного управління особливого значення набуває категорія «забезпечення обороноздатності держави», яку доцільно розглядати як безперервний процес цілеспрямованої діяльності уповноважених суб'єктів, спрямований на формування, підтримання, розвиток і реалізацію оборонного потенціалу та оборонних спроможностей відповідно до визначених цілей державної політики у сфері національної безпеки й оборони. Зазначений процес охоплює стратегічне планування, прогнозування загроз, визначення потреб, ресурсне забезпечення, організацію взаємодії, реалізацію управлінських рішень, моніторинг результатів та коригування заходів відповідно до змін безпекового середовища.

Отже, поняття «оборона», «обороноздатність», «оборонний потенціал», «оборонні спроможності» та «забезпечення обороноздатності» перебувають у тісному взаємозв'язку, проте не є тотожними. Їх розмежування дозволяє визначити місце публічного управління у формуванні обороноздатності держави та створює теоретичне підґрунтя для подальшого дослідження чинників, які впливають на її розвиток в умовах сучасних безпекових викликів.

Таблиця 1.3

Співвідношення основних категорій у сфері забезпечення обороноздатності держави

Категорія	Зміст	Публічно-управлінський вимір
Оборона держави	Сукупність заходів із підготовки та здійснення збройного захисту держави	Організація й реалізація державної політики у сфері оборони
Обороноздатність держави	Здатність держави забезпечувати захист у разі збройної агресії або збройного конфлікту	Цільова характеристика результативності забезпечення оборони
Оборонний потенціал	Сукупність ресурсів і можливостей, які можуть бути використані для оборони	Формування, накопичення, мобілізація та розподіл ресурсів
Оборонні спроможності	Здатність виконувати визначені оборонні завдання за відповідних умов	Планування, розвиток, підтримання та оцінювання спроможностей
Забезпечення обороноздатності	Безперервний процес формування та реалізації необхідних передумов оборони	Стратегічне планування, координація, ресурсне забезпечення, контроль та адаптація

Джерело: систематизовано автором на основі проведених досліджень

Наведена у табл 1.3. систематизація дозволяє встановити функціональний взаємозв’язок між основними категоріями у сфері забезпечення обороноздатності держави. Оборонний потенціал відображає наявні та потенційно доступні ресурси держави, оборонні спроможності характеризують можливості їх практичного використання для виконання визначених завдань, тоді як обороноздатність є комплексною характеристикою здатності держави забезпечувати власний захист. Водночас забезпечення обороноздатності виступає безперервним управлінським процесом, у межах якого здійснюється узгодження відповідних ресурсів, можливостей і заходів. Обороноздатність держави доцільно розглядати не лише як характеристику наявного військового потенціалу, а й як об’єкт цілеспрямованого публічно-управлінського впливу, результативність якого визначається спроможністю відповідних суб’єктів забезпечувати взаємодію військових, економічних, технологічних, інформаційних, кадрових та інших складових. Саме такий підхід створює

передумови для подальшого аналізу історичної еволюції державної політики у сфері оборони України та визначення особливостей трансформації підходів до забезпечення її обороноздатності.

Дослідження обороноздатності держави як об'єкта публічного управління в системі національної безпеки потребує врахування не лише її сутнісних характеристик і структурних складових, а й особливостей історичного становлення відповідної системи управління, бо зумовлено тим, що зміст державної політики у сфері оборони, організація діяльності уповноважених суб'єктів, підходи до стратегічного планування та механізми використання оборонних ресурсів формуються під впливом конкретних історичних, політичних, економічних і безпекових умов. Відтак еволюція обороноздатності України відображає водночас процес становлення її державності, трансформації системи національної безпеки та поступового розвитку інституційної спроможності органів публічного управління забезпечувати збройний захист держави [10].

Історичний досвід України засвідчує, що наявність значного військового потенціалу сама по собі не гарантує належного рівня обороноздатності. Визначального значення набуває здатність держави забезпечити його організаційну цілісність, відповідність актуальним загрозам, ресурсну підтримку та результативне використання. З огляду на це становлення обороноздатності доцільно розглядати крізь призму взаємозв'язку між змінами безпекового середовища, розвитком оборонних інституцій та трансформацією механізмів публічного управління.

У межах нашого дослідження пропонується застосувати комплексний підхід до періодизації становлення та розвитку обороноздатності України, що ґрунтується на поєднанні двох взаємопов'язаних критеріїв: характеру зовнішніх воєнних загроз і змісту організаційно-управлінських перетворень у сфері оборони. На відміну від періодизації, заснованої виключно на змінах чисельності Збройних Сил України, ухваленні окремих нормативно-правових актів або реформуванні військових формувань, зазначений підхід дозволяє простежити

еволюцію ролі держави в організації оборони, розвитку оборонних спроможностей та забезпеченні взаємодії суб'єктів сектору безпеки й оборони.

На підставі зазначених критеріїв доцільно виокремити п'ять основних етапів становлення та розвитку обороноздатності суверенної України (рис. 1.1):

Рис. 1.1. Етапи становлення та розвитку обороноздатності суверенної України

Джерело: систематизовано автором на основі проведених досліджень

Перший етап (1990-1991 рр.) – формування правових і юрисдикційних передумов забезпечення обороноздатності України, можна вважати початковим етапом становлення національної оборонної системи, він був безпосередньо пов'язаний із процесами утвердження державного суверенітету та незалежності України. Його визначальною особливістю стало формування правових передумов переходу від централізованої радянської системи військового управління до власної системи організації оборони, що відповідала б інтересам новоствореної держави.

Важливе значення в цьому процесі мало прийняття Декларації про

державний суверенітет України від 16 липня 1990 р., у якій було проголошено право України на власні Збройні Сили та визначено засадничі орієнтири майбутньої оборонної політики [27]. Документ відображав прагнення до самостійного визначення питань оборони й безпеки та заклав політико-правові передумови для формування національної системи військового управління. Особливістю тогочасного підходу було поєднання прагнення до державного суверенітету із задекларованим наміром у майбутньому стати постійно нейтральною державою та дотримуватися без'ядерних принципів [27].

Із позицій публічного управління значення Декларації полягало насамперед у започаткуванні процесу формування власної компетенції державних інституцій у сфері оборони. До здобуття незалежності військові формування, розміщені на території України, були складовою єдиної радянської системи, а стратегічне планування, розподіл ресурсів і військове командування здійснювалися союзними органами. Тому утвердження державного суверенітету вимагало не лише політичного проголошення права на власну оборону, а й практичного створення організаційних механізмів реалізації цього права.

Принципово новий етап розпочався після ухвалення 24 серпня 1991 р. Акта проголошення незалежності України [102]. Того самого дня Верховна Рада прийняла постанову «Про військові формування на Україні», якою було започатковано підпорядкування військових формувань національним органам влади та створення Міністерства оборони України [73]. Зазначені рішення стали визначальними для становлення державного управління оборонною сферою, оскільки передбачали перехід від зовнішнього централізованого керівництва до формування власної системи прийняття й реалізації оборонних рішень.

Водночас успадковані військові формування були організаційно, матеріально-технічно та функціонально інтегровані до оборонної системи колишнього СРСР. Їхня структура, дислокація, логістичне забезпечення, система підготовки кадрів та організація командування формувалися відповідно до завдань союзного військово-політичного керівництва. За таких умов перед Україною постала необхідність не просто прийняти під національну юрисдикцію

значний військовий потенціал, а здійснити його структурну й функціональну трансформацію відповідно до власних оборонних потреб.

Подальше нормативне оформлення зазначених процесів пов'язане зі схваленням Концепції оборони і будівництва Збройних Сил України 11 жовтня 1991 р. [91]. У документі було визначено загальні засади оборонної спрямованості військового будівництва, підходи до організаційного формування Збройних Сил та основні орієнтири розвитку національної оборонної системи. Із публічно-управлінських позицій значення Концепції полягало у формуванні початкового стратегічного бачення оборонної політики та визначенні напрямів переходу від успадкованої військової організації до власної системи оборони.

Важливою подією стало прийняття 6 грудня 1991 р. законів України «Про оборону України» [97] та «Про Збройні Сили України» [87]. Зазначені нормативно-правові акти заклали законодавчі основи організації оборони, визначили призначення Збройних Сил України та створили правові передумови розмежування компетенції органів державної влади у відповідній сфері.

Підсумовуючи можемо сказати, що перший етап становлення обороноздатності України характеризувався переважанням правових, політичних та організаційно-юрисдикційних перетворень. Його основним результатом стало формування нормативних передумов створення національної системи оборони та започаткування інституційного оформлення державного управління оборонною сферою. Водночас наявність значного успадкованого військового потенціалу ще не означала формування цілісної системи його ефективного використання, оскільки відповідні управлінські, фінансові, кадрові та матеріально-технічні механізми перебували на початковій стадії розвитку.

Під час другого етапу (1992–1996 рр.) відбулося інституційне становлення оборонної системи незалежної України, він характеризувався переходом від нормативного закріплення засад національної оборони до практичного формування інституцій, ресурсних механізмів та організаційних структур, необхідних для забезпечення обороноздатності держави. У цей період основні управлінські зусилля були спрямовані на створення повноцінної системи

військового командування, комплектування Збройних Сил України, організацію матеріально-технічного забезпечення, підготовку військових кадрів та визначення подальшої долі успадкованого військового потенціалу.

Особливістю становлення оборонної системи України було успадкування значних за чисельністю та масштабами військових формувань, запасів озброєння і військової техніки, а також розміщених на її території стратегічних ядерних сил. Водночас їхня наявність супроводжувалася суттєвими організаційними та економічними обмеженнями. Структура успадкованого військового угруповання не повною мірою відповідала потребам оборони незалежної держави, тоді як фінансові можливості України в умовах економічної кризи початку 1990-х років істотно обмежували перспективи його утримання й модернізації.

З огляду на це одним із центральних завдань публічного управління стало забезпечення відповідності між наявними оборонними ресурсами, економічними можливостями держави та визначеними пріоритетами оборонної політики. Практична реалізація зазначеного завдання передбачала реформування організаційної структури Збройних Сил України, створення національної системи військової освіти, розвиток механізмів матеріально-технічного забезпечення, організацію соціального захисту військовослужбовців та вдосконалення нормативного регулювання військової служби.

Важливу роль у цьому процесі відіграло прийняття Закону України «Про загальний військовий обов'язок і військову службу» від 25 березня 1992 р., яким було закладено правові основи проходження військової служби та комплектування військових формувань [72]. Його значення для забезпечення обороноздатності полягало у формуванні нормативних передумов розвитку кадрового потенціалу національної оборонної системи.

Окремим напрямом державної політики цього періоду стало врегулювання питання ядерного роззброєння. Після проголошення незалежності Україна опинилася в складному політико-правовому та безпековому становищі, оскільки на її території перебував значний ядерний арсенал, успадкований від колишнього СРСР. Визначення його подальшої долі вимагало узгодження

внутрішньодержавних пріоритетів, міжнародно-правових зобов'язань, економічних можливостей та потреб національної безпеки.

Важливим етапом цього процесу стало підписання 5 грудня 1994 р. Меморандуму про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї, відомого як Будапештський меморандум [51]. У документі було зафіксовано безпекові запевнення щодо поваги до незалежності, суверенітету та наявних кордонів України. Водночас його положення не передбачали механізму автоматичного військового захисту України в разі збройної агресії.

Проблематика ядерного роззброєння України стала предметом міжнародних наукових дискусій. Зокрема, американський дослідник Дж. Міршаймер у своїй праці «The Case for a Ukrainian Nuclear Deterrent» обґрунтовував позицію щодо доцільності збереження Україною ядерного стримування як засобу протидії потенційним воєнним загрозам [194]. Водночас альтернативні підходи акцентували на міжнародно-правових, економічних, технічних і політичних труднощах збереження відповідного арсеналу.

З позицій публічного управління досвід ядерного роззброєння демонструє складність ухвалення стратегічних рішень у сфері національної безпеки за умов одночасного впливу внутрішніх ресурсних обмежень і зовнішньополітичних чинників. Він також засвідчує необхідність комплексного оцінювання довгострокових наслідків оборонно-політичних рішень, зокрема їхнього впливу на стратегічну автономію держави та наявні механізми стримування воєнних загроз.

Важливим завершальним елементом інституційного становлення національної оборонної системи стало ухвалення Конституції України 28 червня 1996 р. Основний Закон закріпив захист суверенітету й територіальної цілісності України як одну з найважливіших функцій держави, визначив конституційні засади організації оборони та розподілу повноважень між вищими органами державної влади [40].

Особливе значення мало конституційне закріплення статусу Президента

України як Верховного Головнокомандувача Збройних Сил України, повноважень Верховної Ради України у сфері законодавчого забезпечення оборони та відповідальності Кабінету Міністрів України за здійснення заходів щодо забезпечення обороноздатності й національної безпеки [40]. У такий спосіб було сформовано конституційне підґрунтя функціонального розмежування політичного керівництва, законодавчого регулювання та виконавчо-розпорядчої діяльності у сфері оборони.

Отже, другий етап характеризувався поступовим переходом від формування правових передумов оборони до розбудови її інституційного та ресурсного забезпечення. Водночас його результати засвідчили, що ефективність оборонної системи визначається не лише наявністю військових ресурсів, а й відповідністю їхньої структури стратегічним завданням держави, можливостями національної економіки та спроможністю органів державної влади забезпечувати узгоджене управління відповідними процесами.

Третім етапом (1997-2013 рр.) вважаємо інституційний розвиток системи управління обороною в умовах реформування та обмеженості оборонних ресурсів. Розвиток обороноздатності України характеризувався поступовим удосконаленням інституційної структури управління сферою національної безпеки й оборони, формуванням механізмів стратегічного планування, розвитком міжнародного військового співробітництва та здійсненням заходів щодо реформування Збройних Сил України. Водночас зазначені процеси відбувалися в умовах обмеженості фінансових ресурсів, нестабільності оборонної політики та недостатньої узгодженості між задекларованими напрямами реформування й фактичними можливостями їх реалізації.

Особливістю цього періоду стало поступове усвідомлення необхідності переходу від переважно військово-організаційного розуміння оборони до комплексного підходу, який передбачав взаємодію політичних, військових, економічних, інформаційних та інших інструментів забезпечення національної безпеки. Така швидка трансформація зумовлювала підвищення ролі органів державної влади в координації діяльності суб’єктів оборонної сфери, формуванні

стратегічних пріоритетів і забезпеченні відповідності оборонного планування реальним потребам держави.

Важливим кроком у розвитку інституційних засад управління національною безпекою стало прийняття Закону України «Про Раду національної безпеки і оборони України» від 5 березня 1998 р. № 183/98-ВР [103]. Зазначений нормативно-правовий акт визначив правові засади діяльності Ради національної безпеки і оборони України як координаційного органу з питань національної безпеки і оборони при Президентові України, її компетенцію, склад та організаційні основи функціонування.

З позицій публічного управління інституційне закріплення координаційної ролі РНБО України мало принципове значення, оскільки створювало передумови для узгодження діяльності органів виконавчої влади у сфері національної безпеки й оборони. Водночас формування відповідних організаційних структур саме по собі не забезпечувало належної результативності управління, оскільки ефективність їх функціонування залежала від чіткості розмежування повноважень, своєчасності прийняття рішень, достатності ресурсного забезпечення та наявності дієвих механізмів контролю за виконанням визначених завдань.

Подальше нормативно-правове оформлення системи управління національною безпекою було пов’язане з прийняттям у 2003 р. законів України «Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави» [74] та «Про основи національної безпеки України» [99]. Ці нормативно-правові акти визначили важливі засади організації державної політики у сфері національної безпеки, розвитку демократичного цивільного контролю та формування механізмів підзвітності відповідних державних інституцій.

Особливого значення набув розвиток демократичного цивільного контролю, який передбачав забезпечення відповідності діяльності військових формувань і правоохоронних органів конституційним засадам, законодавчим вимогам та визначеним державним пріоритетам. У публічно-управлінському

вимірі зазначений принцип сприяв формуванню передумов для розмежування політичного керівництва, адміністративного управління та військового командування, а також підвищенню прозорості й підзвітності діяльності суб'єктів оборонної сфери.

Водночас практична реалізація відповідних положень супроводжувалася низкою суперечностей. Зокрема, нормативне закріплення принципів демократичного контролю не завжди забезпечувалося належними організаційними механізмами їх реалізації, а реформування системи військового управління відбувалося нерівномірно, тому виникли передумови для виникнення розриву між формально визначеними завданнями оборонної політики та фактичною спроможністю державних інституцій забезпечувати їх виконання.

Одним із провідних напрямів розвитку оборонної системи України впродовж зазначеного періоду стало реформування Збройних Сил України, що передбачало оптимізацію їх чисельності, удосконалення організаційної структури, модернізацію механізмів комплектування, розвиток професійної військової підготовки та поглиблення міжнародного військового співробітництва. Важливу роль у цьому процесі відігравала взаємодія з Організацією Північноатлантичного договору, зокрема в межах програми «Партнерство заради миру», а також участь українських військовослужбовців у міжнародних миротворчих операціях [47].

Зазначені напрями співробітництва сприяли набуттю досвіду спільного планування й проведення операцій, ознайомленню із сучасними підходами до військового управління та поступовому впровадженню окремих процедур і стандартів, поширених у державах-членах НАТО. Однак позитивні результати міжнародної взаємодії не супроводжувалися достатньо послідовним розвитком національного оборонного потенціалу, що значною мірою обмежувало можливості практичного використання отриманого досвіду [47].

Суттєвою проблемою цього періоду залишалася невідповідність між масштабами задекларованих реформ та обсягами фінансового, матеріально-

технічного й кадрового забезпечення їх реалізації. Скорочення чисельності військових формувань, оптимізація організаційних структур і зменшення оборонних витрат не завжди супроводжувалися відповідним підвищенням якісних характеристик оборонних спроможностей. Унаслідок цього процес реформування набував переважно організаційно-кількісного характеру, тоді як питання модернізації озброєння, розвитку військової інфраструктури, підтримання боєготовності та забезпечення належного рівня підготовки особового складу залишалися недостатньо вирішеними [11].

З позицій теорії публічного управління зазначена ситуація засвідчує обмеженість підходу, за якого результативність оборонної політики оцінюється переважно за фактом прийняття нормативно-правових актів, затвердження програм або здійснення організаційних перетворень. Натомість визначальним критерієм ефективності управління обороноздатністю має виступати досягнення конкретних результатів, пов’язаних із формуванням, підтриманням і розвитком оборонних спроможностей відповідно до характеру наявних та прогнозованих воєнних загроз.

У цьому контексті особливого значення набуває взаємозв’язок між стратегічним плануванням, ресурсним забезпеченням та управлінською відповідальністю. За відсутності належної узгодженості між зазначеними елементами навіть розвинена нормативно-правова й інституційна система не гарантує необхідного рівня обороноздатності держави.

Отже, третій етап розвитку обороноздатності України характеризувався формуванням і поступовим удосконаленням інституційних засад управління сферою національної безпеки й оборони, розвитком демократичного цивільного контролю та розширенням міжнародного військового співробітництва. Водночас недостатня послідовність реформ, обмеженість ресурсного забезпечення та невідповідність між стратегічними завданнями й фактичними результатами управлінської діяльності стримували розвиток оборонних спроможностей держави. Зазначений досвід засвідчив необхідність переходу від переважно формального інституційного реформування до результативного управління,

орієнтованого на реальне підвищення обороноздатності.

Передостаннім четвертим етапом (2014–2021 рр.) вважаємо відновлення та розвиток обороноздатності в умовах збройної агресії Російської Федерації проти України у 2014 р., він став визначальним чинником трансформації національної системи забезпечення обороноздатності. Окупація Автономної Республіки Крим і частини територій Донецької та Луганської областей виявила суттєві недоліки попередніх підходів до оборонного планування, ресурсного забезпечення, військової підготовки та організації міжвідомчої взаємодії. Водночас нові безпекові обставини зумовили необхідність прискореного відновлення оборонного потенціалу держави, підвищення боєготовності військових формувань та вдосконалення механізмів публічного управління оборонною сферою.

Особливістю початкового періоду протидії збройній агресії стала необхідність одночасного вирішення оперативних і стратегічних завдань. З одного боку, держава мала забезпечити невідкладне реагування на воєнні загрози, мобілізацію людських і матеріальних ресурсів, відновлення боєздатності військових частин та організацію їх забезпечення. З іншого боку постала потреба в системному перегляді оборонної політики, розвитку інституційної спроможності органів державної влади та формуванні нових підходів до стратегічного планування.

Одним із першочергових управлінських рішень стало проведення часткової мобілізації відповідно до Указу Президента України від 17 березня 2014 р. № 303/2014 [113]. Зазначений захід був спрямований на нарощування чисельності та відновлення спроможностей військових формувань в умовах безпосередньої загрози державному суверенітету й територіальній цілісності України.

Важливим напрямом інституційних перетворень стало відновлення Національної гвардії України відповідно до Закону України від 13 березня 2014 р. № 876-VII [95]. У публічно-управлінському вимірі це рішення відображало необхідність розширення організаційних можливостей держави щодо

забезпечення безпеки й оборони, удосконалення взаємодії між військовими формуваннями та формування додаткових спроможностей реагування на кризові ситуації.

Водночас практика 2014 р. продемонструвала важливість участі громадянського суспільства у забезпеченні обороноздатності держави. Волонтерські організації, громадські ініціативи, представники бізнесу та добровольчі формування відіграли значну роль у забезпеченні військовослужбовців матеріально-технічними засобами, спорядженням, транспортом, медичними ресурсами та іншими необхідними матеріалами [158]. Зазначені процеси засвідчили, що забезпечення обороноздатності не може обмежуватися виключно діяльністю державних органів і військових формувань.

В умовах масштабних воєнних загроз особливого значення набуває спроможність держави організовувати взаємодію з недержавними суб'єктами, залучати суспільні ресурси та формувати механізми координації зусиль різних учасників оборонної діяльності.

Важливим чинником трансформації оборонної політики стало усвідомлення комплексного характеру сучасних загроз. Російська агресія супроводжувалася застосуванням не лише традиційних військових засобів, а й інформаційного, економічного, політичного та кібернетичного впливу. Зазначені особливості розкрито, зокрема, у колективній монографії заг. ред. В. Горбуліна «Світова гібридна війна: український фронт» [136], у якій проаналізовано багатовимірний характер протистояння та взаємозв'язок воєнних і невоєнних інструментів агресії. Для системи публічного управління це означало необхідність переходу від переважно відомчого реагування на окремі загрози до комплексного забезпечення обороноздатності, що передбачає координацію військової, економічної, інформаційної, технологічної та інших складових державної політики.

Подальший розвиток зазначеного підходу відобразився у прийнятті Концепції розвитку сектору безпеки і оборони України, затвердженої Указом Президента України від 14 березня 2016 р. № 92/2016 [110], та Стратегічного

оборонного бюлетеня України, уведеного в дію Указом Президента України від 6 червня 2016 р. № 240/2016 [107]. Зазначені документи визначили основні напрями реформування сектору безпеки й оборони, удосконалення системи управління, розвитку оборонних спроможностей і наближення відповідних процедур до принципів та стандартів НАТО [143].

Особливого значення набуло впровадження планування на основі спроможностей, яке передбачає визначення необхідних можливостей сил оборони з урахуванням прогнозованих загроз, сценаріїв їх застосування та завдань, що мають виконуватися за відповідних умов. На відміну від підходів, орієнтованих переважно на кількісні параметри військових формувань, планування на основі спроможностей спрямоване на забезпечення відповідності між стратегічними цілями, необхідними ресурсами та очікуваними результатами оборонної діяльності.

Важливим етапом удосконалення системи публічного управління стало прийняття Закону України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII [94]. Зазначений закон визначив основні засади державної політики у сферах національної безпеки й оборони, структуру сектору безпеки і оборони, повноваження відповідних суб'єктів, а також засади демократичного цивільного контролю та планування у відповідній сфері. У публічно-управлінському вимірі його значення полягало у формуванні комплексного нормативного підґрунтя для організації діяльності сектору безпеки й оборони, розмежування функцій політичного керівництва та військового командування, розвитку стратегічного планування й підвищення підзвітності державних інституцій.

Подальша трансформація оборонної політики відобразилася у Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 р. № 392/2020 [105], та Стратегії воєнної безпеки України, затвердженій Указом Президента України від 25 березня 2021 р. № 121/2021 [108].

Особливе значення мало закріплення в стратегічних документах підходів,

орієнтованих на стримування збройної агресії, розвиток стійкості держави та суспільства, удосконалення системи оборонного планування й поглиблення міжнародного безпекового співробітництва. Зазначені положення відображали поступове розширення розуміння обороноздатності як характеристики, що залежить не лише від бойових можливостей військових формувань, а й від здатності державних інституцій, економіки та суспільства забезпечувати тривале функціонування в умовах воєнних загроз.

Важливим напрямом стало формування нормативно-правових засад національного спротиву, а саме прийняття Закону України «Про основи національного спротиву» від 16 липня 2021 р. № 1702-IX [98] створило правові передумови для організації територіальної оборони, руху опору та підготовки громадян України до національного спротиву. У контексті публічного управління розвиток зазначеної системи засвідчив посилення ролі міжсекторальної взаємодії та необхідність узгодження діяльності державних органів, органів місцевого самоврядування, військових формувань і громадянського суспільства у сфері забезпечення обороноздатності.

Отже, четвертий етап характеризувався переходом від переважно інституційного реформування до цілеспрямованого відновлення й розвитку оборонних спроможностей держави в умовах реальної збройної агресії. Його визначальними результатами стали вдосконалення стратегічного планування, розвиток демократичного цивільного контролю, формування передумов планування на основі спроможностей, посилення міжвідомчої взаємодії та розширення участі суспільства в забезпеченні оборони. Водночас подальший розвиток зазначених механізмів вимагав підвищення оперативності управлінських рішень, адаптивності оборонної системи та результативності використання наявних ресурсів.

П’ятим етапом (з 2022 р.) ми вважаємо процес трансформації публічного управління у сфері забезпечення обороноздатності України в умовах повномасштабної війни. Повномасштабне вторгнення Російської Федерації 24 лютого 2022 р. зумовило якісну зміну умов функціонування системи

національної безпеки й оборони України. Масштабність воєнних загроз, висока інтенсивність бойових дій, необхідність тривалого ресурсного забезпечення сил оборони та одночасного підтримання функціонування державних інституцій і національної економіки актуалізували потребу в трансформації підходів до публічного управління обороноздатністю.

Правовою основою функціонування держави в нових умовах стало запровадження воєнного стану відповідно до Указу Президента України від 24 лютого 2022 р. № 64/2022 [71] на підставі положень Закону України «Про правовий режим воєнного стану» [101]. Запровадження особливого правового режиму зумовило необхідність адаптації діяльності органів державної влади, військового командування, військових адміністрацій та інших суб'єктів до виконання завдань в умовах безпосередньої воєнної загрози.

Однією з визначальних особливостей зазначеного етапу стало посилення ролі стратегічної координації та оперативності прийняття управлінських рішень. Забезпечення обороноздатності в умовах повномасштабної війни потребувало узгодженого функціонування органів політичного керівництва, військового командування, центральних органів виконавчої влади, місцевих державних адміністрацій, органів місцевого самоврядування та інших учасників оборонної діяльності [135].

Водночас централізація окремих управлінських процесів не усувала необхідності функціонального розмежування повноважень і відповідальності відповідних суб'єктів. Навпаки, складність воєнних завдань зумовлювала підвищення вимог до чіткості управлінських процедур, своєчасності інформаційного обміну, узгодженості рішень та забезпечення контролю за їх виконанням.

Особливого значення набуло формування інтегрованого підходу до використання оборонних ресурсів, що передбачає координацію діяльності Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення, розвідувальних органів та інших суб'єктів сектору безпеки й оборони [139]. За таких умов обороноздатність держави дедалі

виразніше виявляється як результат функціонування складної міжвідомчої системи, ефективність якої залежить від здатності забезпечувати узгодження стратегічних цілей, ресурсів і практичних дій [8].

Важливим напрямом трансформації стало посилення мобілізаційної складової забезпечення обороноздатності. Проведення мобілізаційних заходів, організація комплектування військових формувань, розвиток системи підготовки особового складу та забезпечення його необхідними ресурсами вимагали постійної координації між органами державної влади, військовими структурами, підприємствами й установами. Правові засади відповідних процесів визначаються, зокрема, Законом України «Про мобілізаційну підготовку та мобілізацію» [93]. З позицій публічного управління зазначені процеси відображають перехід до комплексної мобілізації державного та суспільного потенціалу, за якої обороноздатність забезпечується не лише безпосередньою діяльністю сил оборони, а й функціонуванням економіки, системи освіти, охорони здоров'я, транспорту, енергетики, інформаційної інфраструктури та інших сфер суспільного життя.

Вагому роль у забезпеченні обороноздатності України відіграла міжнародна військова, фінансова, матеріально-технічна та гуманітарна підтримка. Взаємодія з державами-партнерами, міжнародними організаціями та багатосторонніми форматами співробітництва зумовила необхідність розвитку спеціалізованих механізмів координації міжнародної допомоги, визначення пріоритетних оборонних потреб, узгодження процедур постачання та забезпечення ефективного використання отриманих ресурсів [20].

Управлінський зміст зазначених процесів полягає в необхідності поєднання внутрішньодержавного оборонного планування із зовнішніми джерелами ресурсного забезпечення, що потребує високого рівня міжвідомчої взаємодії, інформаційно-аналітичного супроводу та стратегічного прогнозування.

Окремого значення в умовах повномасштабної війни набув розвиток оборонно-промислового комплексу та технологічних інновацій. Зростання

потреб сил оборони в сучасних системах озброєння, безпілотних комплексах, засобах радіоелектронної боротьби, інформаційно-комунікаційних технологіях та інших високотехнологічних рішеннях актуалізувало необхідність удосконалення державної політики у сфері оборонного виробництва, науково-технологічного розвитку та інноваційної діяльності [139].

Зазначені процеси засвідчили поступове посилення ролі технологічної складової обороноздатності, що потребує не лише розвитку відповідних виробничих потужностей, а й формування дієвих механізмів взаємодії між державою, науковими установами, оборонними підприємствами, приватним сектором та безпосередніми користувачами новітніх технологій.

Водночас інтенсифікація технологічного розвитку супроводжується зростанням обсягів інформації, необхідної для стратегічного й оперативного управління, підвищенням складності управлінських завдань та скороченням часу, доступного для прийняття обґрунтованих рішень. За таких умов особливого значення набуває розвиток інформаційно-аналітичної складової публічного управління, спрямованої на забезпечення своєчасного отримання, оброблення, систематизації та використання інформації в процесах оборонного планування, ресурсного забезпечення й координації діяльності відповідних суб'єктів [138].

Важливою особливістю сучасного етапу є також необхідність поєднання оперативності управлінських рішень із дотриманням принципів законності, підзвітності та результативного використання державних ресурсів. Специфіка воєнного стану зумовлює застосування особливих процедур управління, обмеження доступу до окремих категорій інформації та підвищення вимог до захисту відомостей оборонного характеру. Водночас зазначені обставини не усувають потреби в забезпеченні належного контролю, запобіганні зловживанням і формуванні механізмів оцінювання результативності управлінської діяльності.

Отже, п'ятий етап становлення та розвитку обороноздатності України характеризується переходом до функціонування оборонної системи в умовах

тривалої повномасштабної війни, що потребує високого рівня адаптивності державних інституцій, комплексної мобілізації ресурсів, розвитку міжвідомчої та міжсекторальної взаємодії, а також прискореного впровадження технологічних інновацій. У цих умовах особливого значення набуває спроможність системи публічного управління забезпечувати безперервність управлінських процесів, оперативне реагування на зміни безпекового середовища та своєчасне коригування оборонної політики відповідно до актуальних потреб держави.

Проведений історичний аналіз дозволяє простежити послідовну трансформацію підходів до забезпечення обороноздатності України (табл. 1.4.), що відображає зміну не лише характеру воєнних загроз, а й змісту публічно-управлінської діяльності у сфері національної безпеки й оборони. Якщо на початкових етапах державотворення пріоритетного значення набували формування правових засад оборони, створення відповідних інституцій та організація управління успадкованим військовим потенціалом, то в подальшому основна увага поступово зміщувалася до розвитку оборонних спроможностей, стратегічного планування, міжвідомчої координації та підвищення результативності використання наявних ресурсів.

Таблиця 1.4

Еволюція підходів до публічного управління забезпечення обороноздатності України

Етап	Особливості забезпечення обороноздатності	Домінуючі управлінські завдання
1990–1991 рр. Правове становлення	Утвердження суверенітету, формування правових засад оборони	Встановлення національної юрисдикції, започаткування військового будівництва
1992–1996 рр. Інституційне становлення	Створення національної оборонної системи, реорганізація успадкованого військового потенціалу	Формування органів управління, ресурсне та кадрове забезпечення
1997–2013 рр. Реформування	Розвиток оборонних інституцій, міжнародне співробітництво, обмеженість ресурсів	Інституційне реформування, стратегічне планування, цивільний контроль
2014–2021 рр. Відновлення спроможностей	Протидія збройній агресії, реформування сектору безпеки й оборони	Мобілізація ресурсів, планування на основі спроможностей, міжвідомча координація

Продовження таблиці 1.4

Етап	Особливості забезпечення обороноздатності	Домінуючі управлінські завдання
З 2022 р. Адаптація до повномасштабної війни	Комплексна мобілізація, міжнародна підтримка, технологічні інновації	Адаптивне управління, інтеграція ресурсів, оперативне прийняття рішень

Джерело: сформовано автором на основі власних досліджень

Водночас еволюція системи забезпечення обороноздатності України не мала виключно поступального характеру. Окремі періоди характеризувалися невідповідністю між задекларованими стратегічними пріоритетами та фактичними можливостями їх реалізації, що зумовлювало виникнення організаційних, ресурсних та інституційних обмежень. Зазначене підтверджує, що формування оборонного потенціалу, розвиток оборонних спроможностей і забезпечення обороноздатності не є автоматично взаємопов'язаними процесами, а потребують цілеспрямованого управлінського впливу.

На сучасному етапі зазначений взаємозв'язок набуває особливого значення, оскільки забезпечення обороноздатності держави здійснюється в умовах високої динамічності безпекового середовища, обмеженості окремих видів ресурсів, зростання складності управлінських завдань та необхідності оперативного реагування на нові загрози. За таких обставин результативність публічного управління визначається не лише здатністю державних інституцій формувати відповідні оборонні ресурси, а й спроможністю забезпечувати їх узгоджене використання, своєчасний перерозподіл, розвиток необхідних спроможностей та адаптацію управлінських рішень до змін воєнно-політичної обстановки.

Отже, історична еволюція забезпечення обороноздатності України засвідчує поступове розширення змісту публічно-управлінської діяльності від правового та організаційного забезпечення функціонування оборонної системи до комплексного управління її ресурсами, спроможностями й розвитком. Зазначене формує теоретичні передумови для розгляду обороноздатності

держави як складного, багатокомпонентного об’єкта публічного управління, функціонування та розвиток якого залежать від взаємодії сукупності внутрішніх і зовнішніх чинників.

З огляду на результати проведеного теоретичного та історичного аналізу виникає необхідність систематизації структурних складових обороноздатності держави та чинників, що визначають особливості її формування й розвитку. У цьому контексті доцільно розмежовувати зазначені категорії, оскільки структурні складові характеризують основні функціональні сфери забезпечення обороноздатності, тоді як чинники відображають внутрішні та зовнішні умови, що сприяють або перешкоджають формуванню відповідних оборонних спроможностей.

На основі проведеного дослідження пропонується виокремлювати такі взаємопов’язані складові обороноздатності держави: військову, економічну, матеріально-технічну, науково-технологічну, інформаційно-аналітичну, кадрову, суспільно-мобілізаційну та організаційно-управлінську. Кожна із зазначених складових має власне функціональне призначення, однак їхній вплив на загальний рівень обороноздатності визначається не лише індивідуальними характеристиками, а й результативністю взаємодії в межах цілісної системи забезпечення національної безпеки.

Особливе місце в запропонованій систематизації посідає організаційно-управлінська складова, яка забезпечує взаємозв’язок між іншими складовими обороноздатності шляхом стратегічного планування, прогнозування, координації, ресурсного забезпечення, організації виконання управлінських рішень, моніторингу та контролю. Її значення полягає у створенні управлінських передумов для перетворення наявного оборонного потенціалу на практичні оборонні спроможності, необхідні для виконання завдань із захисту суверенітету, територіальної цілісності та незалежності держави.

Водночас формування й розвиток зазначених складових відбуваються під впливом сукупності чинників, серед яких доцільно виокремлювати воєнно-стратегічні, політико-правові, економічні, науково-технологічні, інформаційні,

кадрові, суспільні, міжнародно-безпекові та організаційно-управлінські. Зазначені чинники характеризуються взаємозалежністю та динамічністю, що зумовлює необхідність їх комплексного врахування під час формування й реалізації державної оборонної політики.

Ураховуючи наведене, пропонується розглядати обороноздатність держави в публічно-управлінському вимірі як комплексний об'єкт публічного управління в системі національної безпеки, що характеризується здатністю держави забезпечувати цілеспрямоване формування, розвиток, координацію та результативне використання військових, економічних, технологічних, інформаційних, кадрових та інших ресурсів і спроможностей відповідно до характеру безпекових загроз і стратегічних пріоритетів держави.

Забезпечення обороноздатності держави при цьому доцільно розглядати як цілеспрямований, безперервний та адаптивний процес публічного управління, що охоплює оцінювання безпекового середовища, визначення оборонних потреб, формування й розподіл ресурсів, розвиток необхідних спроможностей, координацію діяльності відповідних суб'єктів та оцінювання результативності реалізованих заходів.

На основі узагальнення теоретичних положень щодо сутності обороноздатності держави, її структурних складових та особливостей публічно-управлінського забезпечення розроблено концептуальну модель публічно-управлінського забезпечення обороноздатності держави (рис. 1.2), яка відображає взаємозв'язок основних елементів цього процесу та передбачає можливість адаптивного коригування управлінських рішень відповідно до змін безпекового середовища.

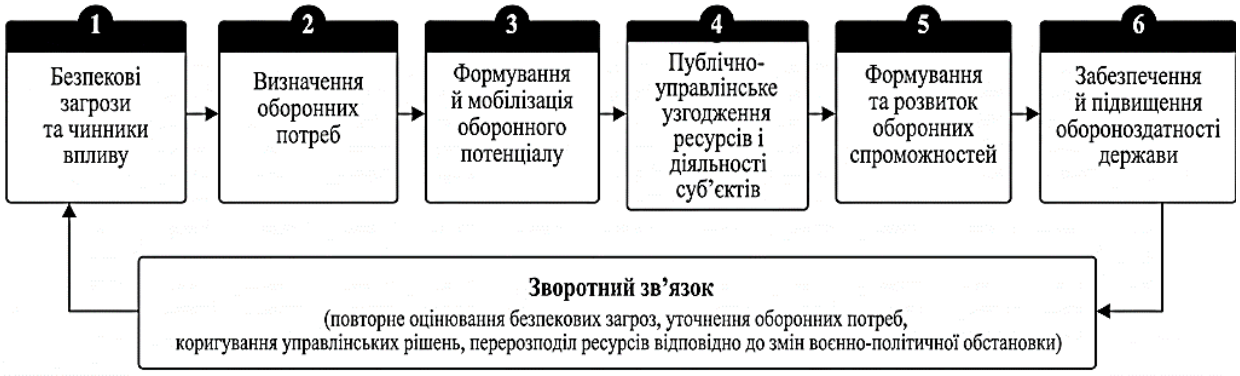

Рис. 1.2. Концептуальна модель публічно-управлінського забезпечення обороноздатності держави

Джерело: авторська розробка

Представлена на рис. 1.2 концептуальна модель відображає послідовність взаємопов'язаних процесів, починаючи з оцінювання безпекових загроз і визначення оборонних потреб та завершуючи формуванням оборонних спроможностей і підвищенням обороноздатності держави. Її визначальною особливістю є виокремлення публічно-управлінського узгодження ресурсів і діяльності відповідних суб'єктів як інтегрувальної ланки між формуванням оборонного потенціалу та розвитком оборонних спроможностей. Передбачений моделлю зворотний зв'язок забезпечує можливість повторного оцінювання загроз, уточнення оборонних потреб, коригування управлінських рішень і перерозподілу ресурсів відповідно до змін воєнно-політичної обстановки. Це дозволяє обґрунтувати необхідність комплексного й адаптивного підходу до публічного управління забезпечення обороноздатності держави.

Отже, обороноздатність держави доцільно розглядати не лише як результат накопичення військового та іншого оборонного потенціалу, а як інтегральну характеристику спроможності держави забезпечувати його організоване, цілеспрямоване й адаптивне використання для виконання завдань оборони. Запропонований підхід створює теоретико-методологічне підґрунтя для подальшого дослідження можливостей удосконалення публічного управління обороноздатністю України, зокрема шляхом використання сучасних інформаційно-аналітичних технологій та штучного інтелекту.

1.3. Теоретичні підходи до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони

Використання штучного інтелекту в системі публічного управління набуває особливого значення в умовах цифрової трансформації та ускладнення безпекового середовища. Для забезпечення обороноздатності держави принциповим є не сам факт упровадження технологій, а їх здатність підвищувати якість аналізу інформації, прогнозування, планування, координації та контролю. У зв'язку з цим особливого значення набуває визначення управлінських можливостей штучного інтелекту, інституційних умов його застосування та взаємозв'язку з формуванням оборонних спроможностей держави.

Штучний інтелект є ключовим компонентом цифрової трансформації сучасного державного управління. Згідно з Організацією економічного співробітництва та розвитку, система ШІ – це машинна система, яка для конкретних або неявних цілей робить висновки на основі вхідних даних та створює результати, такі як прогнози, контент, рекомендації або рішення, здатні впливати на фізичне або віртуальне середовище [205]. Зазначена концепція зосереджена не лише на технологічній природі ШІ, але й, перш за все, на його здатності аналізувати інформацію, виявляти закономірності та генерувати результати, які можуть бути використані людиною або безпосередньо впливати на окремі процеси [205]. Водночас штучний інтелект не слід ототожнювати з традиційною автоматизацією: тоді як системи на основі правил та роботизована автоматизація процесів здебільшого виконують заздалегідь визначені людські інструкції на основі логіки «якщо-тоді», системи машинного навчання можуть обробляти дані, знаходити закономірності та робити прогнози без необхідності планувати всі можливі дії заздалегідь [205].

Важливість штучного інтелекту в державному управлінні визначається тим, що його використання потенційно трансформує не лише окремі технологічні процеси, але й підходи до організації діяльності уряду, розробки політики та взаємодії між державою та громадянами. ОЕСР розглядає

підвищення продуктивності та ефективності внутрішніх процесів, удосконалення процесів прийняття рішень та прогнозування, персоналізацію та оптимізацію державних послуг, а також посилення підзвітності, моніторингу та виявлення незвичайних подій як основні сфери застосування штучного інтелекту в управлінні [171]. Штучний інтелект може бути використаний для обробки великих обсягів неструктурованої інформації, виявлення нових соціальних викликів, оцінки потенційних наслідків політичних рішень, моделювання різних сценаріїв, підтримки реалізації політики та моніторингу її ефективності [227].

На відміну від суто технічного опису ШІ, управлінський підхід вимагає визначити, на яких етапах підготовки та реалізації рішень застосовуються інтелектуальні інструменти та які обмеження супроводжують їх використання.

Використання штучного інтелекту в державному управлінні передбачає поступову трансформацію традиційної моделі обробки інформації та прийняття управлінських рішень у бік більш динамічної моделі, що базується на даних та прогнозах. У той час як класичний управлінський цикл охоплює збір інформації, аналіз посадовцями, підготовку та реалізацію управлінського рішення, а також подальший моніторинг його результатів, використання ШІ дозволяє доповнити цей процес інтелектуальною обробкою великих обсягів даних, створенням моделей, прогнозів, розробкою рекомендацій та постійним моніторингом результатів [215]. Тому штучний інтелект не завжди означає передачу повноважень щодо прийняття управлінських рішень алгоритмам, а насамперед посилення аналітичних, прогностичних та інформаційних можливостей зацікавлених сторін у державному управлінні.

Згідно з «Перспективами цифрового урядування 2026» ОЕСР, штучний інтелект вже використовується майже в усіх країнах ОЕСР принаймні в одній сфері державної діяльності, головним чином для оптимізації внутрішніх процесів та покращення надання державних послуг. Водночас ОЕСР наголошує на важливості переходу від експериментального та пробного використання штучного інтелекту до масштабного, систематичного та відповідального використання [205]. Зазначений перехід включає не лише технологічне

впровадження відповідних рішень, але й розвиток інституційного потенціалу, забезпечення належного управління даними, розвиток цифрової інфраструктури та професійних навичок державних службовців, а також удосконалення механізмів державних закупівель та фінансування. Трансформаційний потенціал штучного інтелекту залежить не лише від наявності відповідної технології, але й, перш за все, від здатності державних установ інтегрувати її в існуючу систему управління та адаптувати організаційні процеси до нових можливостей [56].

Особливо актуальною в цьому контексті є Рамкова програма ОЕСР щодо надійного ШІ в управлінні, яка базується на трьох взаємопов'язаних компонентах: фактори сприяння, бар'єри безпеки та зобов'язання [205]. Перший компонент охоплює основні умови та інституційні можливості, необхідні для впровадження штучного інтелекту, включаючи належне управління, якісні дані, цифрову інфраструктуру, професійні навички та людські ресурси, інвестиції, ефективні механізми державних закупівель та співпрацю з недержавними суб'єктами. Другий компонент – бар'єр безпеки – включає систему запобіжних заходів, розроблених для забезпечення законності, безпеки, прозорості, підзвітності та належного управління ризиками, пов'язаними з використанням штучного інтелекту. Третій компонент, залучення, включає участь громадян, представників бізнесу, наукових спільнот, громадянського суспільства та інших зацікавлених сторін у розробці та вдосконаленні підходів до використання штучного інтелекту [205].

Відповідно, наявність технологічних рішень сама по собі не гарантує підвищення результативності управління. Необхідні належна якість даних, організаційна готовність установ, компетентність персоналу та процедури оцінювання ризиків.

Важливим аспектом використання штучного інтелекту в системі публічного управління є формування належних організаційних та інституційних механізмів оцінювання ризиків, контролю й забезпечення підзвітності. Показовими в цьому контексті є результати досліджень Організації економічного співробітництва та розвитку, відповідно до яких у 14 із 36

досліджених країн (39 %) передбачено обов'язкове оцінювання ризиків перед упровадженням систем штучного інтелекту, у 12 країнах (33 %) функціонують внутрішні механізми колегіального розгляду питань їх використання, а в 11 країнах (31 %) здійснюється аудит після впровадження таких систем [205]. Наведені показники свідчать про нерівномірність інституціоналізації механізмів управління ризиками використання штучного інтелекту в публічному секторі. Для сфери безпеки і оборони це актуалізує необхідність поєднання технологічних можливостей штучного інтелекту з процедурами оцінювання ризиків, забезпеченням інформаційної безпеки, людського контролю та відповідальності за прийняття управлінських рішень.

На основі узагальнення наукових положень та міжнародних підходів доцільно систематизувати п'ять взаємопов'язаних підходів до використання ШІ в публічному управлінні: інструментальний, аналітико-прогностичний, інституційно-управлінський, ризик-орієнтований та адаптивний. Представлена систематизація є авторським аналітичним упорядкуванням відомих підходів, а не твердженням про їх первинне відкриття.

Інструментальний підхід ґрунтується на розумінні штучного інтелекту як технологічного засобу підвищення ефективності та результативності управлінської діяльності. У межах цього підходу основна увага приділяється використанню ШІ для автоматизації повторюваних операцій, опрацювання великих обсягів інформації, формування аналітичних матеріалів, оптимізації адміністративних процесів і підтримки діяльності посадових осіб.

Визначальною особливістю інструментального підходу є підпорядкованість технологічних можливостей штучного інтелекту цілям і завданням публічного управління, під час впровадження відповідних систем та має оцінюватися не лише за технічними показниками швидкодії або точності оброблення інформації, а насамперед за їх здатністю сприяти виконанню управлінських функцій та досягненню визначених результатів державної політики.

У секторі безпеки і оборони інструментальний підхід дозволяє розглядати

ШІ як засіб удосконалення інформаційного забезпечення діяльності органів управління, автоматизації окремих процедур планування, аналізу оборонних потреб, опрацювання даних щодо наявних ресурсів та підготовки управлінських рішень [56]. Водночас застосування таких технологій не змінює правової природи управлінських повноважень, які залишаються за відповідними державними органами та уповноваженими посадовими особами.

Аналітико-прогностичний підхід передбачає розгляд штучного інтелекту як засобу поглиблення інформаційно-аналітичного забезпечення публічного управління шляхом виявлення закономірностей, оцінювання тенденцій, прогнозування можливого розвитку подій і моделювання альтернативних управлінських сценаріїв [60].

На відміну від інструментального підходу, який акцентує увагу на функціональному використанні технологій для виконання визначених завдань, аналітико-прогностичний підхід зосереджується на можливостях формування нової аналітичної інформації, необхідної для підготовки та обґрунтування управлінських рішень. Його застосування створює передумови для переходу від переважно реактивного реагування на вже сформовані проблеми до проактивного управління, орієнтованого на завчасне виявлення ризиків і прогнозування їх можливих наслідків.

У межах зазначеного підходу використання ШІ може охоплювати взаємопов’язані процеси збирання та інтеграції даних, їх аналітичного опрацювання, виявлення закономірностей, оцінювання поточної ситуації, прогнозування, моделювання сценаріїв та формування рекомендацій для суб’єктів управління. Водночас результати алгоритмічного аналізу мають підлягати перевірці, інтерпретації та оцінюванню з урахуванням достовірності вихідних даних, обмежень застосованих моделей і можливих наслідків управлінських рішень.

Особливого значення аналітико-прогностичний підхід набуває в секторі безпеки і оборони, де управлінська діяльність здійснюється в умовах невизначеності, динамічної зміни загроз і необхідності оперативного

використання різнорідної інформації. У зазначеній сфері ШІ може застосовуватися для аналізу безпекового середовища, виявлення потенційних загроз, оцінювання ризиків, прогнозування потреб в оборонних ресурсах, моделювання можливих сценаріїв та підтримки стратегічного й оборонного планування [114].

Отже, аналітико-прогностичний підхід розкриває потенціал штучного інтелекту щодо посилення здатності системи публічного управління своєчасно виявляти зміни безпекового середовища, оцінювати їх наслідки та формувати обґрунтовані управлінські рішення, при цьому ШІ виступає складовою інформаційно-аналітичного забезпечення управлінського процесу, а не самостійним суб'єктом прийняття публічно-владних рішень.

Інституційно-управлінський підхід передбачає розгляд використання штучного інтелекту в контексті організаційних умов, управлінських процедур, компетентності персоналу та інституційної спроможності органів публічної влади [140]. Відповідно до цього підходу результативність застосування ШІ визначається не лише характеристиками технологічних систем, а й здатністю державних інституцій забезпечувати їх інтеграцію в управлінські процеси.

ОЕСР виокремлює серед основних передумов надійного застосування штучного інтелекту в державному секторі належне управління, якісні дані, цифрову інфраструктуру, професійні компетентності, інвестиційне забезпечення, ефективні закупівельні процедури та партнерську взаємодію [205]. Сукупність зазначених умов формує інституційну основу, без якої використання ШІ може залишатися фрагментарним і не забезпечувати очікуваного управлінського результату.

Для сектору безпеки і оборони інституційно-управлінський підхід набуває особливого значення з огляду на необхідність міжвідомчої координації, забезпечення сумісності інформаційних систем, захисту критично важливих даних, розмежування повноважень та організації відповідального використання технологій. Відповідно, впровадження ШІ має супроводжуватися розвитком управлінських процедур, кадрових компетентностей, технологічної

інфраструктури та механізмів взаємодії між суб'єктами сектору безпеки і оборони.

Ризик-орієнтований підхід ґрунтується на необхідності співвіднесення умов застосування штучного інтелекту з характером і масштабом потенційних негативних наслідків його використання. Його сутність полягає у визначенні диференційованих вимог до розроблення, впровадження, експлуатації та контролю систем ШІ залежно від рівня ризику, який вони можуть створювати для людини, суспільства, державних інституцій і безпекового середовища.

Одним із прикладів нормативного закріплення ризик-орієнтованого підходу є Регламент Європейського Союзу 2024/1689 про встановлення гармонізованих правил щодо штучного інтелекту (EU AI Act) [159]. Його положення передбачають диференціацію вимог до систем ШІ, зокрема встановлення спеціальних обов'язків щодо високоризикових систем, пов'язаних з управлінням ризиками, якістю даних, технічною документацією, прозорістю, людським наглядом, точністю, надійністю та кібербезпекою.

Водночас необхідно враховувати особливості сфери застосування зазначеного Регламенту. Системи штучного інтелекту, які використовуються виключно для військових, оборонних або цілей національної безпеки, за встановлених Регламентом умов виключаються зі сфери його дії. Тому положення EU AI Act не можна безпосередньо ототожнювати з нормативними вимогами до всіх систем ШІ оборонного призначення. Разом із тим закладена в ньому логіка пропорційності управлінських і контрольних заходів характеру потенційних ризиків має методологічне значення для розроблення національних підходів до відповідального використання ШІ у сфері безпеки і оборони [210].

З позицій публічного управління ризик-орієнтований підхід передбачає, що посилення технологічних можливостей має супроводжуватися відповідним удосконаленням процедур оцінювання ризиків, перевірки результатів роботи систем, кіберзахисту, людського контролю та визначення відповідальності. Особливого значення це набуває в умовах, коли помилки алгоритмічних систем або використання недостовірних даних можуть спричиняти суттєві наслідки для

оборонного планування, розподілу ресурсів та виконання завдань національної безпеки.

Адаптивний підхід передбачає здатність системи публічного управління своєчасно реагувати на технологічні зміни, трансформацію безпекових загроз, виникнення нових ризиків та результати практичного використання штучного інтелекту. У межах цього підходу управлінські процедури не розглядаються як незмінні, а підлягають періодичному перегляду й коригуванню на основі моніторингу, оцінювання результативності та зворотного зв'язку.

Застосування адаптивного підходу передбачає послідовне здійснення планування використання технологій, попереднього оцінювання ризиків, тестування, впровадження, моніторингу результатів, аудиту та подальшого коригування відповідних організаційних і управлінських процедур. Така послідовність дозволяє поєднувати впровадження технологічних інновацій із необхідністю забезпечення безпеки, підзвітності та стабільності функціонування державних інституцій.

У секторі безпеки і оборони адаптивний підхід має особливе значення, оскільки зміни воєнно-політичної обстановки, характеру загроз, технологічних можливостей і потреб оборонної системи можуть вимагати оперативного перегляду управлінських рішень. Відповідно, використання штучного інтелекту має забезпечувати не лише підготовку аналітичних прогнозів, а й можливість систематичного оцінювання їх достовірності, уточнення вихідних даних та вдосконалення процедур підтримки управлінських рішень.

Отже, розглянуті теоретичні підходи не є взаємовиключними, оскільки характеризують різні сторони використання штучного інтелекту в системі публічного управління. Інструментальний підхід розкриває його технологічне призначення, аналітико-прогностичний показує можливості інформаційно-аналітичного забезпечення управлінських рішень, інституційно-управлінський вказує на організаційні передумови застосування, ризик-орієнтований трактує вимоги до безпеки й контролю, адаптивний має здатність управлінської системи коригувати власну діяльність відповідно до змін середовища. Їх комплексне

поєднання створює теоретичну основу для визначення місця штучного інтелекту в публічному управлінні забезпечення обороноздатності держави.

Практичне значення розглянутих теоретичних підходів особливо виразно проявляється в системі публічного управління сектором безпеки і оборони, де використання штучного інтелекту пов'язане з необхідністю забезпечення оперативності, обґрунтованості та узгодженості управлінських рішень в умовах трансформації характеру воєнних загроз, розвитку цифрових технологій і зростання значення інформаційної переваги застосування ШІ, що поступово виходить за межі автоматизації окремих операцій та охоплює ширше коло процесів стратегічного планування, аналізу безпекового середовища, управління ресурсами й розвитку оборонних спроможностей.

Отже, зазначені підходи характеризують різні, але взаємопов'язані сторони застосування ШІ: інструменти, аналітичні функції, організаційні передумови, ризики та механізми адаптації (табл 1.5).

Таблиця 1.5

Теоретичні підходи до використання ШІ в публічному управлінні сектором безпеки і оборони

Підхід	Зміст	Значення для обороноздатності
Інструментальний	Автоматизація та підтримка управлінських процедур	Опрацювання даних, підготовка рішень
Аналітико-прогностичний	Аналіз тенденцій, ризиків і сценаріїв	Прогнозування загроз та оборонних потреб
Інституційно-управлінський	Умови впровадження, компетентності, координація	Сумісність систем, міжвідомча взаємодія
Ризик-орієнтований	Пропорційний контроль і оцінювання ризиків	Безпека, надійність, підзвітність
Адаптивний	Моніторинг та коригування процедур	Реагування на зміни безпекового середовища

Джерело: систематизовано автором на основі проведеного аналізу

У сфері безпеки й оборони зазначені у табл. 1.5. підходи набувають прикладного значення через можливість застосування ШІ в процесах аналізу безпекового середовища, планування, координації та управління ресурсами.

Порівняльний аналіз сучасних підходів до використання штучного

інтелекту в публічному управлінні свідчить про різні напрями теоретичного осмислення його управлінського потенціалу. Зокрема, у дослідженнях ОЕСР основну увагу приділено інституційним передумовам упровадження ШІ, формуванню належних механізмів управління, забезпеченню прозорості, підзвітності та контролю ризиків. У стратегічних документах НАТО використання штучного інтелекту розглядається насамперед у контексті розвитку оборонних спроможностей, забезпечення оперативної сумісності, відповідального застосування технологій та протидії загрозам, пов'язаним із їх використанням. Водночас у наукових дослідженнях публічного управління окрему увагу приділено організаційній готовності державних інституцій до впровадження інтелектуальних технологій [217].

Узагальнення зазначених положень дозволяє розширити їх застосування до дослідження публічно-управлінського забезпечення обороноздатності держави. Особливістю запропонованої систематизації є поєднання інструментального, аналітико-прогностичного, інституційно-управлінського, ризик-орієнтованого та адаптивного підходів у межах єдиного аналітичного представлення, орієнтованого на процеси визначення оборонних потреб, узгодження діяльності суб'єктів управління, ресурсного забезпечення, формування та розвитку оборонних спроможностей. На відміну від відокремленого розгляду технологічних можливостей, організаційних передумов або безпекових обмежень використання ШІ, запропоноване узагальнення передбачає їх комплексне врахування відповідно до завдань публічного управління забезпечення обороноздатності держави.

Однією з ключових сфер практичного використання штучного інтелекту є безпека й оборона, де його впровадження безпосередньо зумовлене трансформацією сучасних загроз, підвищенням швидкості опрацювання інформації та потребою ухвалювати управлінські рішення за умов значної невизначеності. Тут показовою є позиція НАТО, яке сприймає штучний інтелект не тільки як самостійний технологічний засіб, а і як технологію, спроможну змінити безпекове середовище, військовий потенціал та підходи до протидії

гібридним загрозам. У Стратегії НАТО зі штучного інтелекту на 2021 рік наголошено, що розвиток штучного інтелекту позначається на всіх напрямах діяльності Альянсу, зокрема на колективній обороні, кризовому управлінні та спільній безпеці [217].

У цьому контексті одним із ключових напрямів застосування ШІ є опрацювання великих масивів даних і розвідувальної інформації. Алгоритмічні системи можуть оперативно обробляти різноманітні інформаційні потоки, виявляти взаємозв'язки та закономірності, які складно встановити за допомогою традиційних методів, а також формувати структуровану інформаційну картину для потреб управління. У своїй Стратегії щодо ШІ на 2024 рік НАТО підкреслює важливість поєднання ШІ з високоякісними даними, адже їх наявність і належне управління є необхідною передумовою розроблення безпечних, надійних та ефективних систем штучного інтелекту [201].

Окремої важливості набуває застосування ШІ у сфері логістики та управління ресурсами, в оборонній системі значна кількість управлінських процедур стосується визначення потреб, розподілу ресурсів, організації постачання й прогнозування необхідних спроможностей. Автоматизоване опрацювання даних може застосовуватися для встановлення потреб, оптимізації розподілу ресурсів і передбачення ймовірних змін у них [212]. У такому разі ШІ виступає не лише технологічним інструментом, а й складовою підвищення результативності управлінських процесів у секторі безпеки та оборони.

Особливої уваги набуває протидія гібридним загрозам та інформаційним операціям, бо Стратегія НАТО 2024 року вперше окремо зарахувала до проблем, що викликають занепокоєння Альянсу, використання ШІ з метою поширення дезінформації та здійснення інформаційних операцій. НАТО також підкреслює важливість стратегічного прогнозування й аналітичної роботи для протидії ворожому застосуванню штучного інтелекту [202].

Аналіз стратегічних документів НАТО щодо розвитку та використання штучного інтелекту дозволяє виокремити взаємопов'язані пріоритети його інтеграції у сферу безпеки і оборони, серед яких забезпечення відповідального

розроблення та застосування інтелектуальних технологій, прискорення їх упровадження в процеси формування й розвитку оборонних спроможностей, зміцнення оперативної сумісності, управління технологічними ризиками та протидія загрозам, пов’язаним із використанням штучного інтелекту потенційними противниками [201]. З позицій публічного управління зазначені пріоритети свідчать про необхідність поєднання технологічного розвитку з удосконаленням управлінських процедур, міжвідомчої координації, інституційного забезпечення та механізмів відповідального використання штучного інтелекту в інтересах обороноздатності держави.

1. Забезпечити НАТО та державам-членам можливість слугувати взірцем і сприяти відповідальній розробці та застосуванню штучного інтелекту в інтересах оборони й безпеки союзників.

2. Прискорити та скоординувати інтеграцію штучного інтелекту у створення й реалізацію спроможностей, зміцнюючи оперативну сумісність як ключовий елемент Альянсу, зокрема через упровадження сценаріїв використання штучного інтелекту.

3. Забезпечувати захист і контроль наших технологій штучного інтелекту, управляти пов’язаними з ними ризиками та зберігати нашу спроможність до інновацій з урахуванням аспектів політики безпеки, зокрема впровадження наших PRU.

4. Виявляти й нейтралізувати загрози, що виникають унаслідок використання штучного інтелекту зловмисниками.

Для публічного управління важливо розрізняти використання ШІ в управлінських процесах та управління самим застосуванням ШІ. У першому випадку йдеться про інформаційно-аналітичну підтримку планування й рішень; а у другому про правила, відповідальність, оцінювання ризиків, людський контроль та аудит.

Подальший розвиток стратегічних засад використання штучного інтелекту у сфері оборони відображено в Цифровій стратегії НАТО (Alliance Digital Strategy), оприлюдненій 13 січня 2026 року. Документ визначає цифрову

трансформацію як складову підвищення оборонних спроможностей Альянсу, передбачаючи розвиток захищеної та сумісної цифрової інфраструктури, використання даних як стратегічного ресурсу, інтеграцію інтелектуальних технологій у процеси підтримки управлінських рішень і вдосконалення взаємодії людини з автоматизованими системами. Особливе значення має передбачене Стратегією поєднання технологічної модернізації з удосконаленням цифрового врядування, управління ризиками, професійної підготовки персоналу та оцінювання результативності впроваджених рішень. Відбувається процес становлення важливого підґрунтя для обґрунтування комплексного механізму публічного управління використання штучного інтелекту з метою підвищення обороноздатності України [200].

Стрімке розгортання окреслених підходів зумовлює потребу перейти від використання штучного інтелекту в управлінні до управління самим штучним інтелектом. Йдеться про створення системи AI governance, що включає правила, інституції, процедури, стандарти й механізми контролю, необхідні для безпечного та відповідального розроблення і застосування AI-технологій.

Водночас інституційна система управління ШІ має передбачати комплекс запобіжників (guardrails), спрямованих на запобігання та зменшення ризиків. OECD підкреслює важливість поєднання технологічного розвитку з відповідними політиками, прозорістю, підзвітністю та наглядовими механізмами на всіх етапах життєвого циклу AI-систем. У 2026 році OECD також звертає особливу увагу на потребу посилення попередньої оцінки ризиків, внутрішнього контролю та аудиту AI-систем після їх упровадження у державному секторі [205].

Національний контекст застосування ШІ визначається, зокрема, Концепцією розвитку штучного інтелекту в Україні, схваленою розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р. [111], та планом заходів з її реалізації на 2025–2026 роки, затвердженим розпорядженням Кабінету Міністрів України від 9 травня 2025 року № 457-р. [80].

Особливо важливим є те, що план безпосередньо впливає використання

технологій штучного інтелекту в обороні. Зокрема, відповідальними сторонами є Міністерство оборони України, апарат РНБО, Державна адміністрація спеціального зв'язку та Фонд інноваційного розвитку. Серед заходів – впровадження оборонного планування, яке має гарантувати використання технологій штучного інтелекту в оборонній сфері. Крім того, план передбачає розробку правової бази у сфері штучного інтелекту, розробку рекомендацій щодо кібербезпеки, особливо щодо захисту моделей машинного навчання від несанкціонованого втручання, та прийняття кількох міжнародних стандартів ISO/IEC у сфері штучного інтелекту як національних стандартів. Відбувається поступовий перехід України від концептуального визначення необхідності розвитку штучного інтелекту до створення конкретних правових, організаційних, безпекових та стандартизаційних механізмів для його впровадження.

Базовим документом є Концепція розвитку штучного інтелекту в Україні, вона залишається чинною і визначає основні напрямки державної політики у сфері розвитку та використання штучного інтелекту в Україні. Більш важливим для характеристики поточного етапу реалізації цієї державної політики є план заходів щодо реалізації концепції розвитку штучного інтелекту в Україні на 2025-2026 роки, де загальні умови концепції вже перетворені на конкретні заходи, що визначають відповідальних осіб, терміни та показники ефективності.

Використання штучного інтелекту в системі публічного управління сектором безпеки і оборони потребує узгодженої діяльності суб'єктів, наділених відповідними повноваженнями щодо формування та реалізації державної політики, стратегічного й оборонного планування, ресурсного забезпечення, цифрової трансформації та контролю. Особливого значення в цьому контексті набуває взаємодія Кабінету Міністрів України, Міністерства оборони України, інших центральних органів виконавчої влади, органів військового управління та суб'єктів, відповідальних за забезпечення кібербезпеки, розвиток цифрових технологій та інноваційної діяльності. При цьому функціональна взаємодія зазначених суб'єктів має ґрунтуватися на чіткому розмежуванні повноважень,

узгодженості управлінських процедур, належному інформаційному забезпеченні та визначенні відповідальності за результати використання технологій штучного інтелекту.

З позицій публічного управління інтеграція штучного інтелекту в діяльність сектору безпеки і оборони має розглядатися не як відокремлений процес технологічної модернізації, а як складова вдосконалення управлінської діяльності, спрямованої на забезпечення обороноздатності держави. Зокрема, це передбачає поєднання технологічних можливостей ШІ з організаційними, правовими, кадровими, інформаційними та ресурсними умовами його застосування, а також забезпечення взаємодії суб'єктів управління на різних рівнях прийняття рішень. За таких умов використання штучного інтелекту може сприяти підвищенню узгодженості управлінських дій, обґрунтованості оборонного планування та результативності процесів формування й розвитку оборонних спроможностей держави.

З огляду на модель, обґрунтовану в підрозділі 1.2, використання ШІ доцільно пов'язати з публічно-управлінським узгодженням оборонних потреб, ресурсів та діяльності відповідних суб'єктів. У цьому процесі можна виокремити п'ять функціональних напрямів: інформаційно-аналітичний, прогностичний, планувально-ресурсний, координаційний та контрольно-моніторинговий.

Виокремлені функціональні напрями використання штучного інтелекту в публічному управлінні забезпечення обороноздатності держави мають взаємопов'язаний і взаємодоповнювальний характер, оскільки охоплюють послідовні та взаємозалежні процеси інформаційного забезпечення, прогнозування, планування, координації та оцінювання результатів управлінської діяльності. Інформаційно-аналітичний напрям забезпечує формування інформаційної основи для оцінювання безпекового середовища, наявного оборонного потенціалу та визначення актуальних управлінських потреб. Прогностичний напрям спрямований на передбачення змін безпекових загроз, моделювання можливих сценаріїв розвитку ситуації та обґрунтування перспективних оборонних потреб. Планувально-ресурсний напрям передбачає

використання аналітичних можливостей ШІ для підтримки визначення пріоритетів оборонного планування, оцінювання ресурсних потреб та обґрунтування управлінських рішень щодо формування й розвитку оборонних спроможностей.

Координаційний напрям охоплює інформаційно-аналітичну підтримку узгодження діяльності суб'єктів сектору безпеки і оборони, забезпечення своєчасного обміну інформацією та підвищення узгодженості управлінських дій. Контрольно-моніторинговий напрям спрямований на систематичне відстеження виконання управлінських заходів, оцінювання їх результативності, виявлення відхилень від визначених цілей та підготовку пропозицій щодо коригування управлінських рішень. У сукупності зазначені напрями створюють передумови для посилення аналітичної, прогностичної, організаційної та координаційної спроможності системи публічного управління.

Взаємозв'язок визначених функціональних напрямів дозволяє розглядати використання штучного інтелекту як складову вдосконалення публічно-управлінського забезпечення обороноздатності держави. Його потенційний вплив на підвищення обороноздатності має опосередкований характер і реалізується через підвищення якості та своєчасності управлінських рішень, удосконалення оборонного планування, раціоналізацію використання ресурсів, посилення міжвідомчої взаємодії та забезпечення адаптивності управлінських процесів відповідно до змін безпекового середовища. При цьому результативність застосування ШІ залежить від належної якості даних, інституційної спроможності суб'єктів управління, забезпечення інформаційної та кібербезпеки, людського контролю й відповідальності за прийняті рішення.

Особливістю запропонованого функціонального узагальнення є встановлення взаємозв'язку між основними напрямами використання штучного інтелекту, управлінськими процесами забезпечення обороноздатності та формуванням і розвитком оборонних спроможностей держави. Відповідно, можемо визначити не лише можливі сфери застосування інтелектуальних технологій, а й їх місце в системі публічно-управлінського забезпечення

обороноздатності держави.

Концептуальне відображення взаємозв'язку зазначених функціональних напрямів представлено на рис. 1.3.

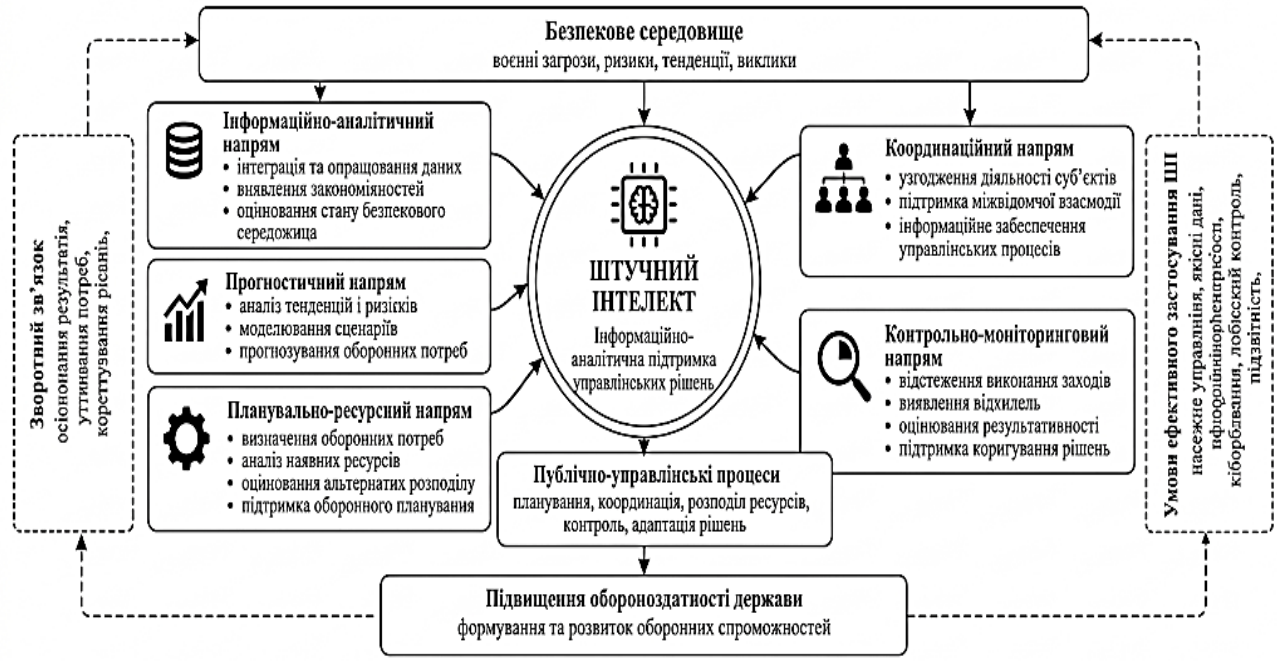

Рис. 1.3. Функціональні напрями використання штучного інтелекту в публічному управлінні забезпечення обороноздатності держави

Джерело: власна розробка автора

Наведена схема відображає взаємозв'язок між застосуванням ШІ, основними управлінськими процесами та підвищенням обороноздатності. ШІ розглядається як інструмент підтримки управлінських рішень, а не як автономний суб'єкт публічної влади. Зворотний зв'язок забезпечує можливість повторного оцінювання результатів, уточнення потреб і коригування заходів відповідно до змін безпекового середовища.

Проведений аналіз теоретичних підходів до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони дозволяє встановити, що результативність застосування інтелектуальних технологій визначається не лише їх технічними можливостями, а й характером інтеграції в управлінські процеси, інституційною спроможністю відповідних суб'єктів, належним ресурсним забезпеченням та ефективністю механізмів контролю. На

основі узагальнення наукових положень та міжнародних підходів систематизовано інструментальний, аналітико-прогностичний, інституційно-управлінський, ризик-орієнтований та адаптивний підходи, комплексне застосування яких створює теоретичне підґрунтя для розгляду штучного інтелекту як інструменту підтримки публічно-управлінських рішень у сфері забезпечення обороноздатності держави.

Обґрунтовано доцільність виокремлення інформаційно-аналітичного, прогностичного, планувально-ресурсного, координаційного та контрольно-моніторингового напрямів використання штучного інтелекту в публічному управлінні забезпечення обороноздатності держави. Їх взаємопов'язане застосування створює передумови для підвищення обґрунтованості та своєчасності управлінських рішень, удосконалення оборонного планування, забезпечення раціонального використання ресурсів, посилення міжвідомчої координації та розвитку оборонних спроможностей. Водночас визначено, що необхідними умовами результативного використання ШІ є забезпечення належної якості даних, інституційної спроможності суб'єктів управління, інформаційної та кібербезпеки, управління ризиками, людського контролю, розмежування відповідальності та адаптивного коригування управлінських процедур відповідно до змін безпекового середовища.

Отже, використання штучного інтелекту в публічному управлінні доцільно розглядати як інструмент посилення управлінської спроможності держави, спрямований на вдосконалення процесів формування та розвитку оборонних спроможностей, що становить одну з передумов забезпечення й підвищення обороноздатності України.

Висновки до розділу 1.

Досліджено генезис штучного інтелекту та еволюцію наукових підходів до визначення його сутності, що дозволило встановити поступовий перехід від концепцій відтворення інтелектуальної діяльності людини до формування технологічних систем, здатних здійснювати обчислювальне висновування,

аналізувати інформацію, формувати прогнози, рекомендації та інші результати з різним ступенем автономності. На основі порівняльного аналізу зарубіжних і вітчизняних наукових підходів систематизовано основні напрями розуміння штучного інтелекту, уточнено його співвідношення із суміжними технологічними категоріями та конкретизовано технологічні, функціональні й системні характеристики. Обґрунтовано доцільність розгляду штучного інтелекту з позицій публічного управління як технологічного інструменту інформаційно-аналітичного забезпечення, прогнозування та підтримки прийняття управлінських рішень, що створює теоретико-методологічне підґрунтя для дослідження його використання з метою підвищення обороноздатності України.

У результаті дослідження теоретичних засад обороноздатності держави як об'єкта публічного управління в системі національної безпеки встановлено, що обороноздатність є комплексною характеристикою здатності держави забезпечувати захист суверенітету, територіальної цілісності та незалежності, яка формується внаслідок взаємодії військових, економічних, матеріально-технічних, науково-технологічних, інформаційно-аналітичних, кадрових, суспільно-мобілізаційних та організаційно-управлінських складових. Обґрунтовано необхідність розмежування понять «оборона», «обороноздатність», «оборонний потенціал», «оборонні спроможності» та «забезпечення обороноздатності», що дозволило уточнити зміст і спрямованість публічно-управлінського впливу на процеси формування та розвитку обороноздатності держави.

На основі поєднання критеріїв характеру зовнішніх воєнних загроз та змісту організаційно-управлінських перетворень запропоновано періодизацію становлення й розвитку обороноздатності України, яка охоплює п'ять етапів: формування правових і юрисдикційних передумов національної оборони (1990-1991 рр.); інституційне становлення оборонної системи незалежної держави (1992-1996 рр.); реформування системи оборони в умовах ресурсних обмежень (1997-2013 рр.); відновлення та розвиток оборонних спроможностей в умовах

збройної агресії (2014-2021 рр.); трансформацію системи забезпечення обороноздатності в умовах повномасштабної війни (з 2022 р.). Встановлено, що історична еволюція відповідної системи супроводжувалася поступовим розширенням змісту публічно-управлінської діяльності – від нормативно-правового та інституційного забезпечення оборони до комплексного управління оборонними ресурсами, спроможностями й розвитком.

Удосконалено теоретичний підхід до розгляду обороноздатності держави як об'єкта публічного управління шляхом розмежування її структурних складових і чинників впливу та обґрунтування інтегрувальної ролі організаційно-управлінської складової. Запропоновано концептуальну модель публічно-управлінського забезпечення обороноздатності держави, яка відображає взаємозв'язок між безпековими загрозами, визначенням оборонних потреб, формуванням і мобілізацією оборонного потенціалу, публічно-управлінським узгодженням ресурсів і діяльності суб'єктів, розвитком оборонних спроможностей та підвищенням обороноздатності держави. Визначено, що інтегрувальна роль публічного управління полягає в забезпеченні узгодженого й результативного використання оборонних ресурсів, тоді як наявність зворотного зв'язку створює передумови для адаптації управлінських рішень до змін безпекового середовища.

Доведено на концептуальному рівні, що забезпечення обороноздатності держави не може обмежуватися накопиченням військових та інших ресурсів, а потребує їх цілеспрямованого перетворення на практичні оборонні спроможності через механізми стратегічного планування, координації, ресурсного забезпечення, моніторингу та контролю. Отримані результати створюють теоретико-методологічні передумови для подальшого дослідження використання штучного інтелекту як інструменту вдосконалення інформаційно-аналітичного забезпечення, прогнозування, планування та прийняття управлінських рішень у сфері оборони України.

Систематизовано теоретичні підходи до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони, серед яких

виокремлено інструментальний, аналітико-прогностичний, інституційно-управлінський, ризик-орієнтований та адаптивний. Встановлено, що їх комплексне поєднання дозволяє розглядати штучний інтелект не лише як технологічний засіб автоматизації управлінських процедур, а й як інструмент посилення інформаційно-аналітичної, прогностичної, організаційної та координаційної спроможності системи публічного управління.

На основі проведеного аналізу обґрунтовано доцільність виокремлення п’яти взаємопов’язаних функціональних напрямів використання штучного інтелекту в публічному управлінні забезпечення обороноздатності держави: інформаційно-аналітичного, прогностичного, планувально-ресурсного, координаційного та контрольно-моніторингового. Визначено, що їх застосування створює передумови для підвищення обґрунтованості та своєчасності управлінських рішень, удосконалення оборонного планування, раціоналізації використання ресурсів, посилення міжвідомчої взаємодії та розвитку оборонних спроможностей. Доведено необхідність поєднання технологічних можливостей штучного інтелекту з належним інституційним забезпеченням, управлінням ризиками, інформаційною та кібербезпекою, людським контролем і відповідальністю суб’єктів публічного управління за прийняті рішення.

Розділ ІІ
ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМУ ПУБЛІЧНОГО УПРАВЛІННЯ ОБОРОНОЗДАТНІСТЮ

2.1. Нормативно-правове забезпечення та правове регулювання застосування технологій штучного інтелекту в сфері національної безпеки й оборони.

Застосування ШІ у державному управлінні потребує формування узгодженої державної політики та визначення єдиних підходів до впровадження, використання та розвитку таких технологій [68]. Особливо це стосується сфери обороноздатності держави під час повномасштабної воєнної агресії з боку росії.

Інтеграція штучного інтелекту в систему публічного управління обороноздатністю України вимагає належного нормативно-правового регулювання. Відповідно до конституційних засад правової та демократичної держави (зокрема ст. 19 Конституції України), інтеграція алгоритмічних систем у прийняття стратегічних рішень повинна відбуватися виключно в межах юридичного поля, гарантуючи законність, прозорість і підзвітність діяльності суб'єктів публічного управління в усіх сферах їхньої відповідальності. Вимога правового регулювання ШІ в оборонній сфері набувають особливої актуальності в умовах правового режиму воєнного стану, оскільки високотехнологічне протистояння вимагає чіткого юридичного обґрунтування та легітимізації кожного управлінського рішення.

Правове регулювання функціонування ШІ загалом – складна та багатогранна проблема, оскільки для якісного його втілення необхідно задіяти категоріальний апарат та принципи кількох галузей права: конституційного, адміністративного, права національної безпеки та оборони, міжнародного гуманітарного права, інформаційного і кіберправа, права інтелектуальної власності, а також законодавства про публічні (оборонні) закупівлі та експортний контроль.

В Україні досі не прийнято спеціального закону, який безпосередньо регулював би функціонування ШІ в оборонному секторі. Чинне нормативно-правове регулювання використання ШІ в секторі безпеки та оборони, зазначають українські дослідники, «має переважно рамковий, фрагментарний і реактивний характер, а практичне впровадження технологій ШІ відбувається швидше, ніж формування відповідних правових та інституційних механізмів» [150].

На сьогодні базовим документом державної політики у сфері використання ШІ є Концепція розвитку штучного інтелекту в Україні, схвалена у 2020 році [42]. Саме в ній надається сучасне визначення штучного інтелекту та зазначається, що він є сукупністю інформаційних технологій, використання яких дозволяє виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, створювати та використовувати бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [42].

Це перший фундаментальний документ, який окреслює загальне бачення державної політики в сфері ШІ за пріоритетними напряммами – освіта, наука, економіка, кібербезпека, оборона, інформаційна безпека, держуправління, правове регулювання та етика, правосуддя.

Концепція розвитку штучного інтелекту в Україні розглядає принципи розвитку та використання технологій штучного інтелекту, дотримання яких повністю відповідає принципам Організації економічного співробітництва і розвитку з питань штучного інтелекту. Ці принципи визначають головні напрями діяльності органів публічного управління у сфері забезпечення обороноздатності. Поняття «обороноздатність держави» визначається Законом України «Про оборону України» [97], де зазначається, що обороноздатність «складається з матеріальних і духовних елементів та є сукупністю воєнного, економічного, соціального та морально-політичного потенціалу», а на органи публічного управління покладається обов’язок організовувати роботу, спрямовану на зміцнення обороноздатності держави. Звичайно, на перший план

висуваються питання національної безпеки, суверенітету та сталого розвитку держави. Принципи розвитку та використання технологій штучного інтелекту передбачають дотримання верховенства права, основоположних прав і свобод людини і громадянина, демократичних цінностей; діяльність та алгоритм рішень систем штучного інтелекту повинні відповідати вимогам законодавства про захист персональних даних, а також додержання конституційного права кожного на невтручання в особисте і сімейне життя у зв'язку з обробкою персональних даних [47].

Восени 2023 року Мінцифри презентувало «дорожню карту» регулювання ШІ в Україні [132], а в червні 2024 року в документі «Біла книга з регулювання ШІ в Україні: бачення Мінцифри» [131] було запропоновано дворівневу стратегію адаптації вітчизняного законодавства до європейських норм. Перший етап передбачає запровадження переважно добровільних, інструментів, які допомагають розробникам враховувати вимоги AI Act, полегшують вихід на ринок ЄС, дають змогу тестувати свої ШІ-продукти під наглядом держави, аналізувати вплив ШІ-технологій на права людини та формувати етичні правила для галузей, які використовують ШІ. На другому етапі, після опрацювання результатів зворотного зв'язку зі стейкхолдерами, Мінцифри планує розробити базовий закон про ШІ, максимально гармонізований з європейським AI Act [156].

У 2025 році було розроблено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки [62], у якому визначені заходи впровадження ШІ в різні сектори життєдіяльності суспільства, відповідальні суб'єкти та строки виконання. Так, за забезпечення використання технологій штучного інтелекту у сфері оборони відповідають Міністерство оборони України, Апарат Ради національної безпеки і оборони України, Адміністрація Держспецзв'язку та Фонд розвитку інновацій. Індикатором виконання є заходи оборонного планування, які забезпечать використання технологій штучного інтелекту у сфері оборони.

Улітку 2026 року Мінцифри винесло на громадське обговорення проєкт нової Стратегії розвитку сфери штучного інтелекту в Україні на період до 2030

року та операційного плану на 2026–2028 роки, що має розширити та поглибити підходи до регулювання галузі [64], зокрема, головною метою, визначеною цією стратегією, виступає прагнення України посісти провідні позиції за рівнем застосування штучного інтелекту в державному секторі та обороні [142]. Обговорення тривало до 30 червня 2026 року. За його результатами було опубліковано «ЗВІТ про результати публічного громадського обговорення проекту розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку сфери штучного інтелекту в Україні на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2026-2028 роках» [34]. Стратегія визначає першочергові та далекострокові цілі та завдання, прописує очікувані результати та критерії їхнього досягнення. Зокрема, стратегічна мета №1, зазначена у документі, конкретизується через низку завдань, одним із яких є «Використання систем штучного інтелекту для зміцнення національної безпеки та оборони» [142]. Органи публічного управління здійснюють цілеспрямоване регулювання та нормативне орієнтування суспільства, спрямоване на підвищення обороноздатності держави через інтеграцію AI-технологій.

Стратегія не лише визначає пріоритетні напрямки розвитку штучного інтелекту в оборонній сфері, але юридично закріплює й розширює ті механізми, які держава вже випробувала і продовжує нарощувати. Зокрема, запущено спеціальну програму фінансування штучного інтелекту в сфері оборони та проведення щорічного огляду потреб екосистеми штучного інтелекту з метою коригування оборонних пріоритетів фінансування [142]. Практичним втіленням зазначених стратегічних орієнтирів є, наприклад, діяльність оборонно-технологічного кластера Brave1 [39], який було створено як грантову програму для оборонних стартапів. Діяльність Brave1 базується на Законах України «Про інноваційну діяльність» [88], «Про державну допомогу суб’єктам господарювання» [76], розпорядженнях Кабінету Міністрів України [39] та Положеннях про грантові програми Brave1 [65;66; 67]. Можна зробити висновок, що управління підвищенням обороноздатності відбувається на декількох рівнях: державному, рівні органів виконавчої влади та на рівні окремих суб’єктів

господарської діяльності.

У напрямку покращення фінансування працює й механізм щорічного огляду потреб екосистеми штучного інтелекту з метою коригування оборонних пріоритетів фінансування. Зокрема, таке тестування проводиться за підтримки Міністерства цифрової трансформації України за ініціативи AI-спільноти AI HOUSE та інвестиційної групи Roosh. Наприклад, результати дослідження «AI-екосистема України: таланти, компанії, освіта» [165] показали поточний стан ринку, виділили ключові тренди індустрії, визначили потреби спеціалістів, що стало підґрунтям для прийняття стратегічних рішень на державному рівні. Зокрема встановлено, що в умовах війни найголовнішим пріоритетом для фінансування є оборонні технології (Defence Tech), а саме: фінансування ШІ-інструментів для безпілотних платформ, систем аналізу цілей та радіоелектронної боротьби. Допомагає моніторингу й робота у так званих «регуляторних пісочницях» (Sandbox) [133], інтеграція яких в українську практичну площину відповідає положенням Регламенту ЄС про штучний інтелект (AI Act) [130]. У межах таких середовищ учасники проєкту отримують безкоштовні консультації юристів, технічних фахівців та бізнес-експертів [133], що сприяє мінімізації ризиків, прискоренню виходу на ринок і залученню додаткового фінансування до проєктів.

На сьогодні механізм щорічного огляду потреб та грантового фінансування оборонного ШІ вже реалізується через запуск спеціальних програм підтримки Defense Tech розробок (зокрема, прямого грантового фінансування до 30 млн грн на рік для одного розробника) [39]. Це дозволило прискорити цикл від розробки AI-алгоритмів (комп'ютерний зір для БПЛА, предиктивна аналітика, розпізнавання цілей) до їх кодифікації та допуску до експлуатації у Силах безпеки і оборони України.

В рамках реалізації Стратегії створено інноваційну платформу «Фабрика оборонного штучного інтелекту» з метою підтримки компаній, які розробляють системи штучного інтелекту. Практичним втіленням цієї ініціативи став запуск навесні 2026 року першого в Україні центру компетенцій із розвитку та

впровадження військових технологій штучного інтелекту – Defense AI Center «A1», створеного Міністерством оборони України спільно з Мінцифрою за підтримки уряду Великої Британії [175]. Ключовим напрямом діяльності Центру є робота з даними, формування єдиних підходів до їх якості, стандартизації, захисту та використання для навчання AI-моделей. Поряд із цим здійснюється моделювання та розбудова симуляційних середовищ для тестування технологічних рішень, розвиток AI-інфраструктури для їх оперативного розгортання, а також розробка інструментів, готових до безпосередньої інтеграції в бойових підрозділах. Це створює основу для точного аналізу інформації з поля бою, прогнозування дій противника та оперативного вироблення ефективних сценаріїв реагування. Окрему увагу зосереджено на розвитку автономних систем – штучного інтелекту для безпілотних і роботизованих комплексів, який забезпечить роботу без GPS та в умовах радіоелектронної боротьби. Подібні рішення об'єднуються у єдину мережу для виконання бойових завдань із мінімальним залученням людини та збереження життя військових [155].

До січня 2026 року елементом нормативно-правового регулювання викоиристання ШІ-технологій була «Концепція Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року» [41], яка втратила чинність з низки об'єктивних причин. По-перше, відбувся перехід від вузькогалузевого до комплексного державного підходу до регулювання сфери використання ШІ. Якщо Концепція охоплювала регулювання переважно економічного сектору [41], то проєкт Стратегії [142] звертає увагу й на державний сектор, безпеку та оборону, освіту, медицину тощо. По-друге, положення Концепції застаріли внаслідок активного наближення українського законодавства до стандартів Європейського Союзу, зокрема після ухвалення європейського Регламенту про штучний інтелект (AI Act) [130] та орієнтацію на нову архітектуру регулювання, що враховує ризико-орієнтований підхід, етичні стандарти та безпекові вимоги ЄС. По-третє, в умовах повномасштабної війни

відбулася кардинальна переорієнтація державних пріоритетів із необхідністю спрямування основних зусиль на розвиток Defense Tech, забезпечення потреб оборони, інтеграцію AI у Сили безпеки і оборони України та створення спеціалізованих профільних інституцій.

Отже, можна констатувати, що попри всі недоліки національного законодавства у сфері обороноздатності, нормативно-правове регулювання адаптується до нових викликів, технологічних проривів та поступово вдосконалюється. І хоча науковці [5; 150] зазначають відсутність чіткої регуляторної бази ШІ, її фрагментарність і незрілість окремих елементів, наявні тенденції свідчать про перехід від декларативних підходів до практичної розбудови міцного фундамента для створення цілісної національної екосистеми обороноздатності.

Потрібно зазначити, що нормативно-правова база використання штучного інтелекту у всіх галузях суспільного життя співвідноситься із європейськими правовими нормами, оскільки України прагне інтегруватися до європейської спільноти. Підписавши Блетчлійську декларацію [219] на британському саміті AI Safety Summit у листопаді 2023 року, Україна долучилася до міжнародного консенсусу щодо безпеки штучного інтелекту. Документ закріплює партнерські зобов'язання держав у сфері мінімізації технологічних загроз та встановлює вимоги щодо безпечного проєктування, розробки і застосування ШІ-систем [69]. У травні 2024 року на 133-му засіданні Комітету Міністрів Ради Європи було прийнято Рамкову конвенцію Ради Європи про штучний інтелект, права людини, демократію та верховенство права, яка набула статусу першого юридично обов'язкового міжнародного документа, спрямованого на комплексне правове регулювання використання ШІ [128]. Вона охоплює діяльність протягом усього життєвого циклу систем штучного інтелекту (розробка, впровадження, експлуатація), яка може впливати на права людини, демократичні процеси та законність, та визначає цінності та принципи використання штучного інтелекту. 15 травня 2025 року зазначену Рамкову конвенцію підписала Україна [68]. У Конвенції міститься застереження, згідно з яким її дія не поширюється на

питання національної оборони, що особливо важливо для України в умовах воєнного стану. Попри це, підписання Україною Конвенції про ШІ надає можливість досягнення збалансованості між інноваційним розвитком та забезпеченням національної безпеки, оскільки Україна заявила про намір поширювати принципи Конвенції про ШІ на приватний сектор через відповідні заходи, що стимулюватимуть бізнес дотримуватися етичних стандартів. Участь у Конвенції підсилює авторитет України як технологічної держави, що поділяє демократичні цінності та бере участь у формуванні глобального порядку денного регулювання технологій майбутнього [7].

Регламент (ЄС) 2024/1869 [130] є першим прикладом комплексного нормативного акта, який започатковує цілісну наднаціональну систему правових координат для сфери штучного інтелекту. Його ключовим завданням є забезпечення правової визначеності, юридичної передбачуваності, стабільності та дотримання базових європейських цінностей і прав людини в умовах цифрової трансформації [14].

Регламент Європейського Союзу про ШІ [130] закладає стратегічний вектор Європейського Союзу, основними принципами якого є людиноцентричний підхід та запроваджує ризик-орієнтовану модель регулювання, встановлює вимоги прозорості для моделей загального призначення та заборону шкідливих практик. Ця система доповнюється Регламентом Європейського Союзу № 2023/2854 Європейського Парламенту та Ради від 13 грудня 2023 року [209] щодо справедливого доступу до даних та їх використання і Регламентом Європейського Союзу № 2022/868 Європейського Парламенту та Ради від 30 травня 2022 року [208] про європейське управління даними [142]. Data Act [209] має велике значення для сфери ШІ, адже навчання моделей ШІ залежить від доступності великих масивів даних [156]. Digital Services Act [129] не спрямований прямо на ШІ, але регулює використання його алгоритмів у онлайн-платформах. General Data Protection Regulation (GDPR) [182] – один з найвідоміших законів ЄС, який діє з 2018 року та встановлює жорсткі вимоги до обробки персональних даних. Всі системи ШІ, що обробляють

персональні дані, повинні також відповідати нормам GDPR [156].

Початок інституціалізації політики ЄС щодо штучного інтелекту припадає на 2018 рік і пов'язаний із прийняттям Єврокомісією перших програмних документів. Ідеться про Комюніке «Штучний інтелект для Європи» [172] та «Скоординований план щодо штучного інтелекту» [172]. Вказані документи визначили стратегічні пріоритети діяльності ЄС у цій сфері, зокрема: нарощування публічних та приватних інвестицій у розвиток технологій штучного інтелекту; підготовка до соціально-економічних трансформацій, зумовлених впровадженням ШІ; а також забезпечення розвитку інтелектуальних систем із дотриманням етичних принципів, норм права та основоположних цінностей Європейського Союзу [14.

У 2019 році Європейська комісія опублікувала «Етичні настанови щодо надійного штучного інтелекту» (Ethics Guidelines for Trustworthy AI) [181] – документ, який визначає критерії відповідності систем штучного інтелекту європейським стандартам безпеки, прав людини та прозорості.

Ключовим інноваційним чинником визначила штучний інтелект і кандидатка на посаду голови Європейської Комісії Урсула фон дер Ляєн, яка у програмі дій «Союз, який прагне більшого: Моя програма для Європи» [225] зазначає, що цифрові технології, особливо штучний інтелект (ШІ), трансформують світ з безпрецедентною швидкістю та допоможуть знайти рішення для суспільних викликів – від охорони здоров'я до сільського господарства, від безпеки до виробництва.

Важливим етапом у формуванні нормативного регулювання штучного інтелекту в Європейському Союзі стало оприлюднення Європейською Комісією 19 лютого 2020 року програмного документа «Біла книга з штучного інтелекту. Європейський підхід до досконалості і довіри» [226]. Цей документ став рамковою основою для майбутніх законодавчих пропозицій з формування нормативно-правової бази застосування ШІ в Європейському Союзі [50], основою якої повинно стати формування нормативного й етичного середовища, що гарантує безпеку, прозорість, недискримінацію, повагу до основоположних

прав людини та дотримання етичних принципів у процесі розробки й застосування ШІ [14].

Логічним продовженням цих законодавчих ініціатив в галузі штучного інтелекту став Регламент (ЄС) 2024/1689 (AI Act) [130], який є основним нормативно-правовим актом у сфері функціонування ШІ на європейському просторі. Ухвалений у червні 2024 року, Регламент передбачає поетапне набрання чинності його положеннями впродовж 2024-2026 років.

Зокрема, 2 лютого 2025 року набрав чинності І і ІІ Розділ Регламенту Європейського Парламенту та Ради (ЄС) 2024/1689 [130], що знаменувало початок поетапного впровадження законодавчої рамки ЄС у сфері штучного інтелекту та перехід від нормотворчої фази до етапу імплементації, який передбачає поступове введення в дію конкретних норм, інституційних структур і механізмів нагляду [14].

Водночас сучасний міжнародний досвід переконливо доводить, що динамічний розвиток цифрових технологій, зокрема ШІ-технологій, вимагає формування чіткої нормативно-правової бази [126]. Прагнучи до повноцінної євроінтеграції, Україна здійснює послідовні кроки у напрямі адаптації національного законодавства до стандартів ЄС. І сфера застосування ШІ не є винятком. При Комітеті Верховної Ради України з питань цифрової трансформації спільно з Міністерством цифрової трансформації було створено спеціальну робочу групу з правового регулювання штучного інтелекту, до якої увійшло понад 100 осіб, серед яких народні депутати України, представники органів державної влади, громадських організацій, українські та міжнародні експерти з питань штучного інтелекту. Першочерговим завданням робочої групи є розробка профільного євроінтеграційного закону до кінця 2026 року [22;157].

Зазначений проєкт Закону розробляється з урахуванням положень європейського Регламенту (EU AI Act) та адаптується до національних правових і соціально-економічних реалій. Його фундаментальною метою є охоплення повного життєвого циклу ШІ-систем – від початкового проєктування й навчання моделей до їхнього підсумкового аудиту та виведення з експлуатації. Крім того,

документ покликаний чітко розмежувати обов'язки провайдерів і суб'єктів застосування ШІ, гарантувати прозорість функціонування алгоритмів, а також встановити юридичну відповідальність за інциденти, здатні завдати шкоди.

Передбачається, що ця частина закону буде враховувати положення європейського Регламенту (EU AI Act) [130], яка класифікує системи ШІ за чотирма рівнями ризику: системи з мінімальним ризиком – більшість систем штучного інтелекту, таких як спам-фільтри та відеоігри зі штучним інтелектом; системи, що мають ризик недостатньої прозорості, наприклад, чат-боти; системи штучного інтелекту з високим ступенем ризику – медичне програмне забезпечення на основі штучного інтелекту, системи для підбору персоналу; системи з неприйнятним рівнем ризику, наприклад, системи штучного інтелекту, які дозволяють урядам або компаніям проводити «соціальний скоринг». Системи штучного інтелекту з неприйнятним рівнем ризику є явною загрозою основним правам людини і тому заборонені [130]. Такий розподіл штучного інтелекту за рівнями ризику дозволяє визначати особливості правового регулювання в залежності від того, який саме ризик лежить в основі системи штучного інтелекту [33].

Особливу увагу представники робочої групи звертають на правове регулювання системи штучного інтелекту, призначених виключно для військових цілей, оборони та забезпечення національної безпеки [22; 157], оскільки цей аспект використання ШІ є надзвичайно важливим для України, яка перебуває в умовах повномасштабного протистояння та виборює свою незалежність, але Регламент (ЄС) 2024/1689 (EU AI Act) [130] виключає ці аспекти за межі дії цього Регламенту, надаючи можливість державам-членам Європейського Союзу самостійно розробляти власні спеціалізовані нормативно-правові інструменти та етичні рамки для розгортання Defense Tech-рішень.

На сьогодні окремий закон про оборонний ШІ в Україні відсутній, тому прийняття закону про регулювання ШІ є надзвичайно актуальним для України особливо в частині його адаптації до українських безпекових й економічних потреб під час війни. Сьогодні оборонні ШІ-технології підпадають під вимоги

законів України про оборонні закупівлі, державну таємницю, інформаційну безпеку, кібербезпеку, правовий режим інтелектуальної власності та правила експортного контролю. Закон «Про захист персональних даних» встановлює вимоги щодо законності, визначення мети, мінімізації та безпеки оброблення персональних даних [86]. Дотримання цих принципів є фундаментальною умовою правомірності застосування систем штучного інтелекту в оборонній сфері, зокрема під час опрацювання біометричних даних, використання технологій розпізнавання облич, відеоаналітики та геолокації, які можуть стосуватися як військовослужбовців, так і цивільних осіб. Фундаментальні засади обігу даних, з якими працюють алгоритми штучного інтелекту, регулюються Законом України «Про інформацію» [89]. Оскільки технології ШІ функціонують шляхом безперервного збору, опрацювання та аналізу даних, нормативні приписи цього Закону закладають юридичні межі щодо допустимості використання інформаційних масивів для навчання моделей. Крім того, встановлений Законом правовий режим інформації з обмеженим доступом та принципи достовірності й повноти даних є критично важливими для захисту службової таємниці й запобігання алгоритмічним помилкам під час застосування ШІ у військовій сфері. Дані, віднесені до державної таємниці, регулюються спеціальним режимом охорони [78], а їх використання для навчання моделей потребує дотримання вимог щодо доступу, зберігання та передачі, особливо якщо розробку здійснюють приватні компанії або міжнародні партнери. Закон «Про захист інформації в інформаційно-комунікаційних системах» [85] та Закон «Про критичну інфраструктуру» [92] створюють правову основу для визначення вимог до безпеки систем, у яких застосовуються алгоритми ШІ. Закон «Про авторське право і суміжні права» встановив спеціальний режим охорони об’єктів, створених із використанням комп’ютерних програм без безпосередньої творчої участі людини [70]. В оборонній галузі питання інтелектуальної власності охоплюють ширший спектр аспектів: права на програмне забезпечення, моделі, набори даних, результати науково-дослідних робіт, проведених у межах державного замовлення, а також порядок ліцензування та

подальшого вдосконалення відповідних рішень. Недостатня врегульованість цих питань у договорах створює ризик залежності Збройних Сил від одного постачальника та ускладнює масштабування успішних розробок. Закон України «Про оборонні закупівлі» [96] безпосередньо впливає на можливість створення, випробування та прийняття на озброєння технологій штучного інтелекту. Оскільки ШІ-системи належать до високотехнологічних рішень, цей Закон визначає правову рамку для придбання програмних продуктів, послуг з їх розробки, адаптації та технічного супроводу. Водночас регулювання оборонних закупівель у сфері ШІ потребує гнучких механізмів, які б враховували специфіку об'єктів інтелектуальної власності, необхідність безперервного оновлення алгоритмів і навчальних датасетів, а також суворого дотримання режимів секретності на всіх етапах розробки. Порядок контролю за передачею відповідних товарів і технологій регулює Закон «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» [75]. У сфері використання ШІ цей напрям набуває особливої актуальності з огляду на зростання експортного потенціалу українських оборонних розробок і розвиток спільного виробництва з іноземними партнерами.

Але у національному законодавчому полі, зокрема, у спеціальних законах, присвячених регулюванню національної безпеки та оборони, термін «штучний інтелект» не використовується, що ускладнює визначення об'єкта правового регулювання, розподіл відповідальності та формування вимог до таких систем.

Наразі в Україні існує потужне законодавство, яке визначає принципи та засади обороноздатності. Так, Закон України «Про національну безпеку України» окреслює основи державної політики у сфері національної безпеки та оборони, визначає структуру сектору безпеки й оборони, а також закріплює принцип демократичного цивільного контролю за його функціонуванням [94]. Закон «Про оборону України» регулює організацію оборони держави, повноваження органів державної влади, питання військового будівництва та оборонного планування [97]. Водночас Закон «Про Збройні Сили України» визначає призначення, завдання й базові принципи діяльності Збройних Сил [87].

Закон «Про основи національного спротиву» окреслює склад сил оборони, у рамках якого цивільний потенціал, зокрема технологічні можливості, може використовуватися для виконання оборонних завдань [98]. Правові основи функціонування режиму воєнного стану, запровадженого з 24 лютого 2022 року, встановлює Закон України «Про правовий режим воєнного стану» [101], що розширює можливості органів влади щодо мобілізації ресурсів і швидкого ухвалення рішень.

Жоден із зазначених законів безпосередньо не регулює питання застосування штучного інтелекту. Проте вони створюють необхідну правову та інституційну основу, визначаючи органи й установи, відповідальні за розвиток озброєння, проведення науково-технічної політики та впровадження інноваційних технологій.

Важливі нормативно-правові засади використання ШІ задля забезпечення обороноздатності закладає, зокрема, Стратегія національної безпеки України «Безпека людини – безпека країни», яка зараховує технологічний поступ, зміцнення оборонно-промислового комплексу та впровадження передових технологій у секторі безпеки й оборони до ключових складових національної безпеки [105]. Стратегія воєнної безпеки України конкретизує ці напрями для оборонної галузі, наголошуючи на потребі технологічного оновлення озброєння, розвитку систем управління, розвідки та протидії загрозам у кіберпросторі [109].

Стратегічне значення для безпечного розвитку та регулювання ШІ-технологій має кібербезпековий компонент. Стратегія кібербезпеки України [106] та Закон «Про основні засади забезпечення кібербезпеки України» [100] визначають базові засади захисту критичної інформаційно-комунікаційної інфраструктури, від функціонування якої безпосередньо залежить надійність ШІ-систем військового призначення. інформаційно-комунікаційних систем, від функціонування яких залежать військові рішення на основі ШІ: від захисту каналів обміну даними до захисту навчальних масивів даних від ворожого втручання [125].

Однак за відсутності спеціального законодавства правова наука та

юридична практика змушені інтерпретувати вимоги до систем ШІ через призму загальних норм права, що неминуче спричиняє правову невизначеність, а відсутність спеціалізованого нормативно-правового акта або галузевої стратегії застосування ШІ у сфері обороноздатності свідчить про наявність системної прогалини в законодавстві, яка потребує нормативного врегулювання [119].

У цьому контексті розробка Проєкту Закону України «Про правове регулювання штучного інтелекту» має стратегічне значення для оборонної сфери, оскільки формує сферу його дії, систематизує понятійну базу та закріплює базові принципи державного регулювання. Такими принципами наразі є принципи верховенства права, людиноцентричності, технологічності, нейтральності, підзвітності, прозорості, захисту персональних даних та обов'язковості фахового людського контролю [22; 157]. Також Закон визначатиме практики із штучним інтелектом, які можуть завдати шкоди окремим особам або групам людей. До таких практик пропонується віднести використання маніпулятивних методів та техник, прогнозування злочинів, розпізнавання емоцій, біометричну категоризацію за чутливими ознаками та використання дистанційної біометричної ідентифікації в режимі реального часу в громадських місцях (із винятками для правоохоронних та безпекових цілей) [22; 157]. Окрему увагу приділено сектору безпеки й оборони та визначенню меж дії закону під час воєнного стану.

При цьому важливо врахувати те, що у міжнародній доктрині військовий ШІ розглядають не як самостійну різновидність озброєння, а як технологію широкого призначення, здатну інтегруватися в різні системи й процеси [169; 204]. У межах правового аналізу доцільно виокремити такі основні напрями його застосування:

• Аналітичні системи та засоби підтримки ухвалення рішень: обробка розвідувальної інформації, аналіз супутникових зображень і відеопотоків, прогнозування, забезпечення ситуаційної обізнаності, системи управління військами;

• Автономні можливості озброєння та військової техніки: пошук,

виявлення, ідентифікація й відстеження цілі, наведення, а в окремих випадках – її вибір і застосування сили [167; 169];

• Безпілотні й роботизовані повітряні, наземні та морські комплекси, оснащені засобами автоматизованої навігації, розпізнавання об'єктів і кінцевого наведення;

• Кібернетичні та інформаційні засоби: виявлення несанкціонованого доступу, захист мереж, оброблення даних із відкритих джерел, ідентифікація дезінформації;

• Функції забезпечення: логістика, технічне обслуговування, медичний супровід, підготовка особового складу, розмінування.

Важливим питанням правового регулювання є також встановлення норм забезпечення людського нагляду за високоризиковими системами. Рівень автономності систем штучного інтелекту відображає ступінь їхньої самостійності та спроможність функціонувати без прямого втручання людини. У контексті дослідження ШІ, зокрема у військовій сфері, правозахисна організація Human Rights Watch (HRW) та Міжнародна клініка з прав людини Гарвардської юридичної школи (IHRC) класифікують такі системи за критерієм автономності ухвалення критичних рішень, наприклад, виявлення, вибору та враження цілей. На цій підставі виокремлено три категорії роботизованої зброї: «людина в контурі» (Human-in-the-loop), «людина над контуром» (Human-on-the-loop) та «людина поза контуром» (Human-out-of-the-loop) [191]. Зброя категорії «Human-in-the-loop» відрізняється тим, що ШІ виконує лише допоміжну функцію – обробляє дані, виявляє об'єкти, вираховує траєкторію, але остаточну команду про застосування сили завжди дає людина. Системи протиповітряної оборони на кшталт Patriot чи Phalanx належать до категорії «Human-on-the-loop», де ШІ виявляє та захоплює ракети ворога, проте оператор бачить процес і може ним керувати – скасувати дію, перехопити управління. Системи категорії «Human-out-of-the-loop» повністю автономні, вони самостійно знаходять ціль, ухвалюють рішення про її знищення та завдають удару без участі чи підтвердження з боку людини.

Акт ЄС про штучний інтелект [130] враховує рівні автономності ШІ і на цій підставі закріплює обов'язкові вимоги щодо забезпечення людського нагляду за високоризиковими системами. Регламент встановлює, як саме треба навчати операторів, визначає стандарти використання спеціальних запобіжників (kill switches) та встановлює заборони на повне виведення людини з контуру управління. які запобіжники (kill switches) мають бути вбудовані в код і де саме закон повністю забороняє відключати людський контроль. Попри свій регіональний статус, Регламент фактично задає глобальні орієнтири для ризик-орієнтованого регулювання, запобігання зловживанням та етичного розвитку штучного інтелекту [168].

У звіті Human Rights Watch «Losing Humanity: The Case against Killer Robots» [191] підкреслюється, що розробка, виробництво та використання повністю автономної зброї мають бути під цілковитою забороною, а не лише підлягати регулюванню. Обґрунтуванням такої вимоги є теза про те, що функціонування таких систем порушує стандарти міжнародного гуманітарного права, закріплені, зокрема, у Додатковому протоколі I до Женевських конвенцій [30]. Як держава-учасниця Женевських конвенцій 1949 року та Додаткового протоколу I до них, Україна несе міжнародно-правове зобов'язання забезпечувати суворе дотримання норм міжнародного гуманітарного права під час розробки та впровадження нових засобів ведення війни, зокрема високоризикових систем штучного інтелекту військового призначення. Особливого значення у цьому контексті набуває стаття 36 Додаткового протоколу I, яка зобов'язує держави на етапах дослідження, розроблення, придбання або прийняття на озброєння нових видів зброї, засобів чи методів ведення війни визначати, чи підпадає їх застосування під заборони міжнародного права [30]. У сфері штучного інтелекту це передбачає проведення комплексної правової експертизи, предметом якої мають бути не лише апаратні комплекси («залізо»), а й програмне забезпечення, алгоритми, навчальні датасети та специфіка експлуатаційних умов. Додатковим гуманітарним запобіжником виступає застереження Мартенса (ст. 1 Протоколу I), яке імперативно

наголошує: навіть за відсутності спеціалізованих нормативних актів цивільні та військові особи залишаються під захистом принципів гуманності та вимог суспільної свідомості [30].

Аналогічну жорстку позицію займає Стокгольмський інститут дослідження проблем миру (SIPRI) [141]. Організація наполягає на прийнятті юридично закріплених обов'язкових міжнародних норм щодо заборони систем зброї, що діють поза контуром людського контролю, та обмеження алгоритмів ШІ для вибору та ураження цілей. У дослідженнях SIPRI наголошується, що збереження людського контролю є критичною умовою для забезпечення дотримання принципу запобіжності та правової відповідальності під час застосування військових інновацій. Така позиція визначає, що законність автономних систем забезпечується не повною забороною технології як такої, а встановленням чітких обмежень щодо типів цілей, часу й території застосування, масштабів використання, а також можливості людського втручання та припинення роботи системи [167]. Отже, найбільш доцільною основою для національного законодавства повинен стати функціональний підхід, який допоможе встановити ефективне регулювання системам ШІ з урахуванням їхнього призначення, рівня автономності та потенційних ризиків.

Іншим значним багатостороннім проєктом у сфері використання ШІ є Кодекс поведінки Групи семи (G7) [183]. Він закріплює кодекс поведінки диспозитивного характеру, заснований на керівних орієнтирах для розробників передового ШІ, і передбачає формування стратегій ризик-орієнтованого регулювання та необхідність надійних засобів контролю безпеки. Зазначений Кодекс може стати основою кращих міжнародних практик щодо відповідального впровадження інновацій у сфері штучного інтелекту та виступити концептуальною основою для підготовки вітчизняного проєкту закону [168].

Найповніше питання використання ШІ в оборонному секторі опрацьовується в межах Конвенції про заборону або обмеження використання окремих видів звичайної зброї, у рамках якої діє Група урядових експертів з проблематики смертоносних автономних систем озброєння. Схвалені нею у 2019

році керівні принципи підтверджують поширення норм міжнародного гуманітарного права на всі типи озброєнь, наголошують, що рішення про застосування зброї повинна ухвалювати людина, а не машина, і передбачають врахування взаємодії «людина – машина» на всіх етапах життєвого циклу системи [211]. Попри відсутність обов'язкової юридичної сили, ці принципи є важливою основою для вироблення національної політики.

У 2024 році Генеральна Асамблея ООН прийняла резолюцію, присвячену використанню штучного інтелекту у військовій галузі та його впливу на міжнародний мир і безпеку. У цьому документі підтверджено, що норми міжнародного права поширюються на відповідні технології, та започатковано подальше обговорення за участю держав-членів [160].

Натомість ще у 2023 році Сполучені Штати оприлюднили Політичну декларацію про відповідальне використання штучного інтелекту та автономії у військовій сфері. Цей документ визначає систему добровільних заходів та принципів, що охоплюють здійснення правової оцінки озброєнь, забезпечення належного людського контролю під час ухвалення рішень про застосування сили, всебічне тестування й оцінювання систем, а також мінімізацію ризиків виникнення алгоритмічної упередженості [207].

Оскільки членство в НАТО визначено стратегічним пріоритетом України, підходи Альянсу до регулювання ШІ мають слугувати орієнтиром для вітчизняного нормотворення. Стратегія НАТО щодо штучного інтелекту, затверджена у 2021 році й оновлена у 2024 році, визначає ключовими засадами законність, підзвітність, пояснюваність, простежуваність, надійність та керованість алгоритмів [217]. Імплементація цих стандартів у національне законодавство дозволить Україні забезпечити оперативну й технологічну сумісність із силами Альянсу, зокрема під час спільного використання оборонних систем та обміну даними.

При підготовці національного закону варто використати також досвід самітів з безпеки штучного інтелекту, які об'єднують уряди, провідні компанії зі штучного інтелекту та дослідників для обговорення ризиків безпеки штучного

інтелекту та потенційних стратегій їх пом'якшення [168].

Інтеграція міжнародних стандартів та адаптація Регламенту ЄС про штучний інтелект у вітчизняну правову систему мають обов'язково здійснюватися із дотриманням принципу конституційності та верховенства права. Відповідно до статей 6 та 8 Конституції України [40], будь-які законодавчі новації повинні ієрархічно підпорядковуватися Основному Закону. Це забезпечує єдність правового поля держави, запобігає виникненню юридичних колізій, та гарантує захист фундаментальних прав і свобод людини (ст. 3) [40]. Закон про правове регулювання штучного інтелекту [22; 157] не є виключенням і повинен відповідати основоположним засадам Конституції України, яка визначає ціннісні орієнтири, принципи та межі повноважень органів державної влади, відповідно до яких має здійснюватися функціонування ШІ для підсилення обороноздатності країни. Згідно зі статтею 17 Конституції України, основними функціями держави є захист її суверенітету й територіальної цілісності, а також забезпечення державної безпеки [40]. Стаття 65 закріплює оборону Вітчизни як конституційний обов'язок громадян, а стаття 106 наділяє Президента України повноваженнями Верховного Головнокомандувача Збройних Сил і голови Ради національної безпеки і оборони, вибудовуючи систему стратегічного керівництва, у тому числі у сфері новітніх технологій. Водночас Конституція визначає життя, здоров'я, честь і гідність людини як найвищі соціальні цінності (ст. 3), гарантує право на життя (ст. 27), повагу до людської гідності (ст. 28) та недоторканність особистого й сімейного життя (ст. 32) [40]. Саме ці норми повинні стати основою нормативно-правового регулювання використання ШІ в оборонній сфері, закладати підґрунтя для вимог щодо збереження людського контролю при розробці та впровадженні ШІ, гарантування безпеки персональних даних та недопущення необґрунтованого стеження, зокрема під час використання технологій розпізнавання облич і автоматизованого аналізу даних.

У березні 2026 року Міністерство оборони України затвердило Концепцію використання штучного інтелекту в Збройних силах. Вона спрямована на цифрову та технологічну трансформацію армії, зокрема через впровадження

компютерного зору (аналіз даних з БПЛА, розпізнавання цілей) та автоматизацію рішень [35; 147].

За підсумками аналізу нормативно-правової бази використання штучного інтелекту в підвищенні обороноздатності України з позицій публічного управління, варто визначити першочергові заходи для покращення та вдосконалення нормативно-правових засад впровадження штучного інтелекту в секторі безпеки і оборони України.

По-перше, необхідно продовжити роботу над Проєктом Закону України «Про правове регулювання штучного інтелекту», який має стратегічне значення для оборонної сфери, оскільки формує сферу його дії, систематизує понятійну базу та закріплює базові принципи державного регулювання.

По-друге, на рівні національного законодавства уточнити понятійно-категоріальний апарат, а саме: закріпити поняття штучного інтелекту, автономних і напівавтономних систем озброєння, а також рівнів людського контролю, узгодивши їх із міжнародною термінологією.

По-третє, розробити та затвердити галузеву концепцію чи стратегію застосування ШІ у секторі безпеки й оборони, визначивши принципи законності, відповідальності, пояснюваності, надійності, керованості та зменшення упередженості відповідно до міжнародних стандартів та стандартів НАТО.

По-четверте, запровадити механізм правової оцінки нових засобів і методів ведення війни, зокрема, систем штучного інтелекту, визначити уповноважений орган і критерії здійснення такого аналізу.

По-п’яте, встановити уніфіковані стандарти тестування, оцінювання та сертифікації систем ШІ, а також забезпечити обов’язкове документування прийнятих рішень для подальшого аудиту й розслідування.

По-шосте, на законодавчому рівні визначити порядок роботи з даними: встановити класифікацію військових масивів, процедури їх передавання розробникам і партнерам, а також вимоги щодо якості та захисту від несанкціонованого втручання.

По-сьоме, у нормативно-правових актах, які регулюють оборонні закупівлі

та інтелектуальну власність, передбачити типові договірні умови для програмного забезпечення на основі ШІ, зокрема щодо прав на моделі й дані, ліцензування, технічного обслуговування та оновлення.

Потребують вирішення також питання правового статусу даних, які застосовуються для навчання моделей: визначення статусу масивів розвідувальної та бойової інформації, порядку їх передавання розробникам і партнерам, а також механізмів захисту від компрометації. Окремі ризики зумовлені використанням комерційних та іноземних моделей і хмарних сервісів, оскільки це створює залежність від зовнішніх постачальників і потребує договірних та організаційних засобів захисту, а тому цей аспект також потребує окремого правового регулювання та інституційного контролю.

Кібербезпека систем ШІ також вимагає спеціальних вимог, адже традиційні стандарти не охоплюють загроз отруєння даних і змагальних прикладів. Навмисне внесення викривлених або модифікованих даних у тренувальні вибірки на етапі навчання ШІ-моделей у контексті оборонних рішень (зокрема ШІ-платформи «SPECTR» та систем комп’ютерного зору БПЛА) це може призвести до системних помилок у розпізнаванні ворожої техніки, спотворення аналітики ситуаційної обізнаності або хибного процес визначення та передачі точних координат цілі (об’єкта ураження) на вогневі засоби (артилерію, БПЛА, ракетні комплекси, авіацію) для її знищення або подавлення.

Такий підхід підсилить інституційні засади впровадження штучного інтелекту в секторі безпеки і оборони України, зробить функції суб’єктів публічного управління прозорими, підвищить рівень довіри до них з боку суспільства.

2.2. Суб'єкти публічного управління та їх функціональна взаємодія при впровадженні ШІ у сфері обороноздатності

Ефективність імплементації технологій штучного інтелекту в оборонний сектор України безпосередньо залежить від чіткості розподілу повноважень між суб'єктами публічного управління та рівня їхньої функціональної узгодженості. У сучасних умовах інституційна система забезпечення обороноздатності на основі ШІ утворює багаторівневу структуру, де кожен суб'єкт виконує спеціалізовану роль у загальному управлінському циклі.

Інституційна архітектура забезпечення регулювання сферою ШІ-технологій на рівні Європейського Союзу детально описана у Розділі VII AI Act [130] та представлена на рис. 2.1.

Рис. 2.1. Інституційна архітектура забезпечення регулювання сферою ШІ-технологій на рівні Європейського Союзу.

Джерело: створено автором на основі [130]

Центральною виконавчою ланкою в інституційній системі регулювання штучного інтелекту на рівні Європейського Союзу є Європейська Комісія. У її складі в лютому 2024 року створено Офіс штучного інтелекту, який став

центральним координаційним та виконавчим вузлом інституційної системи ЄС, який безпосередньо контролює найпотужніші моделі ШІ загального призначення. Офіс здійснює нагляд та контроль за розробниками моделей ШІ загального призначення, оцінює ризики та розробляє кодекси практики, керівні принципи та технічні стандарти. Іншим інститутом із забезпечення гармонізованого та однакового застосування EU AI Act на всій території ЄС є Європейська рада з питань штучного інтелекту (European Artificial Intelligence Board – AI Board). Це колегіальний координаційний орган ЄС, що складається з високопосадових представників кожної держави-члена ЄС та Європейського інспектора з захисту даних (EDPS). Очолює Раду один із представників держав-членів, а Офіс з ШІ забезпечує її секретаріат. Європейська рада з питань штучного інтелекту надає Європейській Комісії висновки, рекомендації та консультації щодо оновлення списків високоризикових технологій, розробки гармонізованих стандартів та уніфікації правозастосовної практики [156].

Для надання технічної експертизи та консультування Ради та Комісії, а також для сприяння виконанню їхніх завдань, створюється Консультативний форум (Advisory Forum) та Наукова група незалежних експертів (Scientific Panel of Independent Experts). Наукова група незалежних експертів складається з провідних науковців та фахівців з ШІ, обраних Комісією на основі сучасного наукового або технічного досвіду в галузі штучного інтелекту. Вона організовує технічні експертизи, попереджає Офіс з ШІ про виникнення нових системних ризиків (systemic risks) та надає науково обґрунтовані рекомендації щодо класифікації models ШІ. Консультативний форум – це інклюзивний орган, до якого входять представники бізнесу, малого та середнього підприємництва, стартапів, громадянського суспільства, академічних кіл та профспілок. Забезпечує зворотний зв’язок із ринком та експертним середовищем. Агентство з основоположних прав, ENISA, Європейський комітет зі стандартизації (CEN), Європейський комітет зі стандартизації в галузі електротехніки (CENELEC) та Європейський інститут телекомунікаційних стандартів (ETSI) є постійними членами дорадчого форуму [130].

Згідно з EU AI Act, кожна держава-член ЄС повинна призначити або створити національні компетентні органи, які забезпечать правозастосування Регламенту на засадах об'єктивності та високого фахового рівня. Це можуть бути новостворені структури або вже наявні, наприклад, агентства з кібербезпеки, органи сертифікації або органи влади, дотичні до цифрової трансформації, шляхом розширення їхніх повноважень. Ці органи здійснюють ринковий нагляд, реєстрацію високоризикових ШІ-рішень, перевірку їхньої оцінки відповідності, а також опрацьовують скарги та застосовують заходи адміністративного впливу. Обов'язковою умовою є створення органу нотифікації та органу ринкового нагляду. Орган нотифікації відповідає відповідальний за акредитацію та призначення органів оцінки відповідності для високоризикових ШІ-систем, а також за нагляд за діяльністю таких органів. Тобто орган нотифікації сам не сертифікує ШІ-системи, але видає нотифікації (уповноваження) спеціалізованим установам, які будуть проводити оцінку відповідності (аудит, тестування, сертифікацію) ШІ-систем, що підпадають під регулювання AI Act [156].

Отже, інституційна архітектура регулювання сфери штучного інтелекту на рівні Європейського Союзу побудована за наднаціонально-децентралізованим принципом. Вона поєднує централізовані нормативно-наглядові повноваження Європейської Комісії, покладені на спеціалізований Офіс з питань ШІ, щодо фундаментальних моделей загального призначення із децентралізованою системою національних компетентних органів держав-членів, координованих Європейською радою з питань ШІ та підкріплених незалежною науково-експертною експертизою [156].

Приєднання України до Європейської ради зі штучного інтелекту у 2025 році [148] актуалізувало завдання щодо визначення національної системи компетентних органів у цій сфері. У науково-аналітичному дискурсі висловлюються різні підходи до їх формування. Зокрема, С. Юхименко припускає, що функції з оцінки відповідності можуть бути покладені на Національне агентство з акредитації України або на новостворений спеціалізований орган із сертифікації [156]. Водночас у середовищі бізнесу та

громадськості наголошується на необхідності створення саме незалежного регулятора. Зокрема, під час обговорення проєкту Стратегії розвитку сфери штучного інтелекту в Україні на період до 2030 року представники Української асоціації операторів зв'язку «ТЕЛАС» запропонували визначити окремий регуляторний орган у сфері ШІ, який здійснюватиме ринковий нагляд, відповідатиме критеріям ефективності та незалежності згідно зі стандартами ЄС та не дублюватиме повноважень інших органів державної влади [34]. Окремо AI Act зобов'язує кожну державу визначити, які національні публічні органи відповідають за забезпечення дотримання вимог щодо основоположних прав людини при використанні високоризикових ШІ-систем [156].

Модель інституційного забезпечення та функціональні повноваження державних органів у сфері ШІ закладаються в проєкті Закону України «Про правове регулювання штучного інтелекту» [22; 157].

Згідно з проєктом, на Кабінет Міністрів України покладаються функції з формування державної політики, координації уповноважених органів та затвердження базових порядків щодо діяльності регуляторних пісочниць, вимог до суб'єктів оцінки відповідності, а також правил перевірки й післяринкового нагляду за універсальними моделями штучного інтелекту. На Міністерство цифрової трансформації України як головний орган у системі формування та реалізації державної політики у сфері штучного інтелекту покладаються функції з узагальнення законодавчої практики, оприлюднення національних і європейських технічних стандартів, сприяння розробці кодексів практики, підвищення рівня розвитку ШІ-грамотності населення та поглиблення міжнародного співробітництва. Спеціальний цифровий регулятор розроблятиме підзаконні акти й методичні рекомендації, здійснюватиме ринковий нагляд за універсальними моделями штучного інтелекту, погоджуватиме плани регуляторних пісочниць. Органи державного ринкового нагляду здійснюватимуть контроль у конкретних галузях, наприклад, НБУ щодо платіжних систем та фінансового сектору, НКЕК – у сфері електронних комунікацій та поштового зв'язку [22; 157].

Для регулювання штучного інтелекту в секторі безпеки і оборони України у модель інституційного забезпечення варто включити Міністерство оборони України, яке, згідно з Положенням [83], формує та реалізує державну політику у сфері оборони, зокрема забезпечує Збройні Сили, здійснює оборонні закупівлі й організовує науково-технічний супровід. Сьогодні Міністерство оборони України системно сприяє впровадженню штучного інтелекту в Сили оборони, щоб підвищити ефективність ураження ворожих цілей. Так, використання ШІ-платформ для автоматизованої обробки даних розвідки дозволило скоротити час від виявлення до ураження ворожих цілей до 90% [29; 154]. При цьому Україна системно дотримується принципу human-in-the-loop. Крім того, МОУ надало вітчизняним розробникам доступ до розвідувальної платформи Avengers Labs, призначеної для навчання та тренування моделей штучного інтелекту [29].

До інституційної архітектури регулювання штучного інтелекту в підвищенні обороноздатності України потрібно віднести й CERT-UA (Computer Emergency Response Team of Ukraine) – спеціалізований урядовий підрозділ у складі Державного центру кіберзахисту Держспецзв'язку. Основною місією цього органу є реагування на кіберінциденти та кібератаки. Окрім базових функцій кіберзахисту CERT-UA взаємодіє з іншими суб'єктами забезпечення національної безпеки, зокрема, Кіберполіцією, Службою безпеки України, Міністерством оборони та Збройними Силами України, а також представляє Україну в міжнародній мережі команд реагування FIRST (Forum of Incident Response and Security Teams) та здійснює партнерство з кіберпідрозділами країн НАТО і ЄС. Безпосередній зв'язок підрозділу з втіленням штучного інтелекту в систему обороноздатності країни зумовлений його участю в розслідуванні кіберінцидентів у мережах автоматизованих систем управління, безпілотних авіаційних комплексів та геоінформаційних систем оборонного призначення.

Отже, цілісна інституційна архітектура регулювання штучного інтелекту в Україні формується за участю Кабінету Міністрів України як стратегічного координатора, Міністерства цифрової трансформації як головного органу, який формує державну політику у цій сфері, спеціального цифрового регулятора й

органів державного ринкового нагляду, які є незалежними або напівнезалежними регуляторними суб'єктами, а також залученням CERT-UA до кібербезпекового захисту та Міністерства оборони України до впровадження ШІ-технологій у секторі безпеки й оборони, що відповідає потребам прискореної кодифікації оборонних технологій в умовах високої динаміки цифрових інновацій та потребує гнучкого нормативного регулювання (Рис. 2.2).

Рис. 2.2. Інституційна архітектура забезпечення регулювання сфери ШІ на національному рівні

Джерело: створено автором на основі [22; 83; 157]

Як видно з рис.2.2 публічно-управлінська складова регулювання ШІ-технологій охоплює розмежування повноважень між органами державної влади. Водночас використання штучного інтелекту в підвищенні обороноздатності України потребує не лише оновлення та вдосконалення нормативно-правової бази, але й уточнення та конкретизації інституційних засад і взаємодії суб'єктів у секторі безпеки і оборони.

Стратегічні рішення у сфері оборони та безпеки ухвалює Президент України як Верховний Головнокомандувач і голова Ради національної безпеки і оборони [94; 97]; Кабінет Міністрів України забезпечує реалізацію державної політики, зокрема, у сфері безпеки та оборони [90], тоді як Міністерство оборони України формує політику у сферах озброєння, науково-технічної діяльності та оборонних закупівель [83; 87]. Координацію загальнодержавної політики у сфері ШІ здійснює Міністерство цифрової трансформації України [9; 111]. До виконання завдань у сфері кіберзахисту, зокрема, залучаються Служба безпеки України та Державна служба спеціального зв'язку та захисту інформації [81].

Тому доцільно уточнити склад інституційної архітектури забезпечення ШІ на національному рівні (рис. 2.2) з огляду на питання обороноздатності країни. Потрібно зазначити, що суб'єкти публічного управління у сфері забезпечення обороноздатності взаємодіють між собою по вертикалі та по горизонталі, у відповідності до статусу у суспільстві, міри підпорядкування, функціональних обов'язків та повноважень, які вони виконують. При цьому вертикальні зв'язки відображають відносини підпорядкованості, нормотворення та стратегічного контролю, а горизонтальні – оперативну координацію, обмін даними, спільну R&D-діяльність та міжвідомчу синергію. Отже, варто розглянути інституційну архітектуру публічного управління забезпечення ШІ у сфері обороноздатності України за допомогою п'яти взаємопов'язаних функціональних блоків (табл. 2.1 – 2.5).

Так політико-законодавчий блок (табл. 2.1) відображає функціонування вищого рівня публічного управління, на якому відбувається формування стратегічних засад державної політики, законодавче регулювання використання технологій ШІ у сфері оборони, ухвалення нормативно-правової бази та нормативно-бюджетне забезпечення цього процесу.

Таблиця 2.1.

Політико-законодавчий блок

Суб'єкт	**Компетенції у сфері застосування ШІ для оборони**	**Нормативно-правове підґрунтя**
Президент України	Гарант державної незалежності, національної безпеки та Верховний Головнокомандувач Збройних Сил України: визначає стратегічних пріоритетів у сфері оборони й безпеки, затвердження стратегічних документів; очолює Раду національної безпеки і оборони України, в установленому порядку вводячи в дію її рішення; видає укази і розпорядження з питань національної безпеки і оборони.	Конституція України [40]; Закон України «Про національну безпеку України» [94]; Закон України «Про оборону України» [97]; Закон України «Про основи національного спротиву» [98]
Рада національної безпеки і оборони України	координація, контроль, планування та прогнозування з питань національної безпеки та оборони; розроблення і вираження важливих політичних рішень щодо реалізації внутрішньої і зовнішньої політики у сфері національної безпеки і оборони України; виявлення й оцінювання загроз національній безпеці.	Конституція України [40]; Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України [105]; Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України [106]
Верховна Рада України	здійснює парламентський контроль та приймає закони України, які визначають і регулюють діяльність органів сектору безпеки і оборони та їхні повноваження, а також затверджує відповідні бюджетні асигнування та приймає рішення щодо звіту про їх використання. Прийняття базових законів про регулювання ШІ, визначення правового режиму використання технологій у сфері оборони та національної безпеки, законодавчий нагляд.	Закон України «Про національну безпеку України» [94]; Закон України «Про Регламент Верховної Ради України» [104]

Джерело: створено автором на основі [39; 44; 49; 52; 59; 127; 149; 175]

У таблиці 2.2. представлено виконавчо-координаційний блок публічного управління обороноздатністю держави.

Таблиця 2.2.

Виконавчо-координаційний блок

Суб'єкт	Компетенції у сфері застосування ШІ для оборони	Нормативно-правове підґрунтя
Кабінет Міністрів України	Ключовий координаційний та виконавчий суб'єкт забезпечення національної безпеки й обороноздатності України. Реалізація державної політики, ухвалення планів заходів, нормативне регулювання інноваційної діяльності; вирішення тактичних завдань та оперативне, повсякденне управління обороноздатністю. забезпечення державного суверенітету і економічної самостійності України, виконання внутрішньої і зовнішньої політики; здійснення заходів щодо забезпечення обороноздатності і національної безпеки України;	Конституція України [40]; Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України [111]; Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні … : розпорядження Кабінету Міністрів України [80; 81]
Міністерство оборони України та його підрозділ - Центр трансформації процесів управління оборонними ресурсами	Вироблення політики у сферах озброєння, закупівель і науково-технічного поступу; Впровадження передових (інноваційних) технологій у Збройні Сили України, допуск їх до експлуатації та швидка кодифікація. Забезпечення оборонної спроможності: Створення умов для інтеграції ШІ-рішень та роботизованих систем у сектор безпеки й оборони. Центр трансформації процесів управління оборонними ресурсами відповідає за розробку, впровадження та адаптацію цифрових систем [146].	Про затвердження Положення про Міністерство оборони України : постанова Кабінету Міністрів України [83]

Продовження таблиці 2.2.

Суб'єкт	Компетенції у сфері застосування ШІ для оборони	Нормативно-правове підґрунтя
Міністерство цифрової трансформації	забезпечує формування та реалізацію державної політики у сфері цифровізації, цифрового розвитку, цифрових інновацій та штучного інтелекту. Розробка стратегій, концепцій, дорожніх карт розвитку ШІ та нормативно-правових актів у цивільному секторі. Впровадження міжнародних стандартів, етичних принципів використання ШІ, забезпечення балансу між інноваціями та захистом прав громадян. Розвиток людського капіталу, освітніх програм, створення сприятливого середовища для IT-бізнесу та ШІ-розробок. Інтеграція України до європейських та світових ініціатив у сфері регулювання ШІ (зокрема гармонізація з EU AI Act).	Дорожня карта з регулювання штучного інтелекту в Україні [31]; Біла книга з регулювання штучного інтелекту в Україні: бачення Мінцифри [9]; Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України [111]

Джерело: створено автором на основі [39; 44; 49; 52; 59; 127; 149; 175]

На цьому рівні відбувається затвердження та виконання державних цільових програм, міжвідомча координація, формування загальних цифрово-технічних стандартів, нормативне регулювання та закупівля оборонних розробок.

Таблиця 2.3 демонструє суб'єктів публічного управління, які входять до безпеково-інфраструктурного блоку регулювання обороноздатності.

Таблиця 2.3.

Безпеково-інфраструктурний блок

Суб'єкт	Компетенції у сфері застосування ШІ для оборони	Нормативно-правове підґрунтя
Служба безпеки України	уповноважений державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку; Захист критичної інфраструктури та контррозвідка: Запобігання кіберзагрозам, контррозвідувальний захист систем ШІ, що використовуються у сфері оборони, контррозвідки та державного управління. Використання технологій штучного інтелекту (аналіз великих масивів даних, розпізнавання образів, моніторинг інформаційного простору) для контррозвідувальної, оперативно-розшукової діяльності та боротьби з тероризмом. Співпраця з CERT-UA, Держспецзв'язку та іншими суб'єктами Національної системи кібербезпеки для виявлення та нейтралізації складних таргетованих кібератак (APT-груп) на ШІ-інфраструктуру держави.	Закон України «Про основні засади забезпечення кібербезпеки України» [100]; Закон України «Про захист інформації в інформаційно-комунікаційних системах» [84]; Закон України «Про критичну інфраструктуру» [92]
Державна служба спеціального зв'язку та захисту інформації України	уповноважений орган у сфері кіберзахисту, криптографічного та технічного захисту інформації. Формування та реалізація політики кіберзахисту: визначення вимог до безпеки ШІ-систем, які інтегруються в об'єкти критичної інфраструктури та державні інформаційні ресурси. Адміністративне керівництво спеціалізованими підрозділами: забезпечення діяльності Державного центру кіберзахисту та підпорядкованого йому CERT-UA (Computer Emergency Response Team of Ukraine). Захист критичної інформаційної інфраструктури: моніторинг загрозового середовища, забезпечення стійкості цифрових систем і засобів спеціального зв'язку, що використовують ШІ-алгоритми. Нормативно-технічне регулювання та оцінка відповідності засобів захисту інформації та кіберзахисту.	Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» [77]

Продовження таблиці 2.3.

Суб'єкт	Компетенції у сфері застосування ШІ для оборони	Нормативно-правове підґрунтя
Урядова команда реагування на комп'ютерні надзвичайні події України – CERT-UA	забезпечує безпосередній кіберзахист та практичну стійкість цифрової інфраструктури держави. Виявлення, локалізація та усунення наслідків кібератак на державні інформаційні ресурси, об'єкти критичної інфраструктури та ШІ-системи. Моніторинг загрозового середовища: Постійний аналіз аномалій, уразливостей algorithms/моделей ШІ та специфічних векторів атак (наприклад, отруєння даних, спотворення алгоритмів, супротивні атаки — adversarial attacks). Координація та обмін інформацією: Взаємодія з міжнародними командами CSIRT/CERT, вітчизняними суб'єктами кібербезпеки (СБУ, Нацполіція, ЗСУ) для оперативного інформування про кіберзагрози у сфері цифрових технологій.	Закон України «Про основні засади забезпечення кібербезпеки України» [100]; Закон України «Про захист інформації в інформаційно-комунікаційних системах» [84]; Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» [77]; Закон України «Про електронні комунікації» [79]

Джерело: створено автором на основі [49; 44; 52; 175; 39; 149; 59]

Ці суб'єкти публічного управління забезпечують контррозвідувальні заходи щодо цифрових систем, протидію спеціалізованим загрозам ШІ (отруєння даних, змагальні атаки, інверсія моделей), реагування на кіберінциденти та криптографічний/інформаційний захист каналів зв'язку.

Оперативно-застосовний блок (табл. 2.4) здійснює свою діяльність на основі практичного застосування ШІ-систем у бойових умовах. Саме на основі їх практичного використання відбувається формування оперативно-тактичних вимог до ШІ-систем, інтеграція технологій у контури управління військами, практичне застосування на полі бою та забезпечення зворотного зв'язку для донавчання ШІ-моделей.

Таблиця 2.4.

Оперативно-застосовний блок

Суб'єкт	Компетенції у сфері застосування ШІ для оборони	Нормативно-правове підґрунтя
Генеральний штаб	Формування оперативних вимог до новітніх зразків озброєння та військової техніки на основі реального досвіду бойових дій. Безпосереднє впровадження та випробування ШІ-систем у процесах управління військами, безпілотних комплексах, засобах РЕБ та аналізі розвідувальних даних. Формування замовлення для Міністерства оборони України щодо критично необхідних інноваційних рішень та цифрових технологій для фронту.	Закон України «Про основи національного спротиву» [98]; Закон України «Про правовий режим воєнного стану» [101]
Збройні Сили України	практичний споживач, оператор та майданчик для реального бойового застосування технологій штучного інтелекту та цифрових інновацій. Використання ШІ-рішень у бойових умовах (безпілотні системи, засоби РЕБ/РЕР, автоматизовані системи управління військами C4ISR, розпізнавання та аналіз цілей). Тестування інноваційних розробок на полі бою та надання оперативних зауважень для прискореної модифікації алгоритмів і технічних рішень. Прийняття на озброєння та систематичне використання технологій, що пройшли процедуру допуску через Міноборони та відповідно до вимог Генштабу.	Закон України «Про Збройні Сили України» [87]

Джерело: створено автором на основі [49; 44; 52; 175; 39; 149; 59]

Функціональним призначенням інноваційно-технологічного блоку (табл. 2.5) є дослідження та розробка (НДДКР/R&D) у сфері оборонного ШІ, акселерація MilTech-стартапів, створення алгоритмів комп'ютерного зору, автопілотування, аналітика ситуаційної обізнаності та систем C4ISR та інші аспекти цифровізації та запровадження ШІ у різні сфери життєдіяльності суспільства, зокрема, в оборонну сферу.

Таблиця 2.5.

Інноваційно-технологічний блок

Суб'єкт	Компетенції у сфері застосування ШІ для оборони	Нормативно-правове підґрунтя
Оборонний кластер Brave1	ланка між цивільним інноваційним сектором, військовими потребами та державними органами. Пошук, відбір та надання грантової підтримки перспективним розробкам у сфері ШІ та miltech. Оцінка технологічної готовності (TRL) та відповідності розробок реальним оперативним потребам Генерального штабу ЗСУ та Збройних Сил України. Надання підтримки розробникам у проходженні бюрократичних процедур для якнайшвидшого допуску до експлуатації через Міністерство оборони України. Поєднання можливостей розробників Мінцифри/IT-індустрії з практичним бойовим досвідом ЗСУ.	Закон України «Про інноваційну діяльність» [88]; Закон України «Про державну допомогу суб'єктам господарювання» [76]
Defense AI Center «A1»	Перший центр експертизи при Міністерстві оборони України, створений для інтеграції ШІ у військові процеси. перетворення бойових даних на аналітичні інсайти, розробка автономних систем, що працюють без GPS та в умовах РЕБ, а також автоматизація планування операцій.	Defense AI Center «A1» [175]
ШІ-платформа «SPECTR»	Спеціалізована екосистема, що розробляється Центром «A1». автоматизація роботи військових штабів, швидкий аналіз оперативних даних з поля бою та моделювання/прогнозування ймовірних дій противника. розробляє та впроваджує AI-рішення для Збройних Сил: аналіз бойових даних, прогнозування дій противника, автономні системи (БпЛА, наземні роботи, рої), нові засоби командування та управління (C2) і симуляційні середовища. Пілотні проєкти проходять випробування безпосередньо у бойових підрозділах ЗСУ.	ШІ-платформа SPECTR [52]

Джерело: створено автором на основі [49; 44; 52; 175; 39; 149; 59]

Отже, аналіз функціонального призначення інститутів державного управління ШІ дозволив побудувати схему «Інституційна архітектура забезпечення ШІ у сфері обороноздатності України» (рис. 2.3).

Рис. 2.3. Інституційна архітектура забезпечення ШІ у сфері обороноздатності України

Джерело: створено автором на основі аналізу нормативно-правових актів

Ця схема відображає вертикальні та горизонтальні зв'язки, які існують між органами державного управління, військово-політичним керівництвом, цивільними органами, які відповідають за цифрову політику, та інноваційними структурами, які висувають ідеї використання ШІ для підвищення рівня обороноздатності та втілюють їх на практиці. Водночас досі немає чітко визначеного єдиного органу або міжвідомчого механізму, відповідального за ШІ в оборонній сфері, із прозорим розподілом повноважень у питаннях правової оцінки систем, їх сертифікації, нагляду за використанням і оцінювання ризиків.

Інституційна архітектура забезпечення ШІ у сфері обороноздатності України була б неповною без освітнього компоненту. Адже саме він забезпечує підготовку військових операторів, аналітиків ШІ, розробників оборонних програмних продуктів, інженерів, а також фахівців у сфері публічного управління та адміністрування, які відповідають за забезпечення та регулювання процесів впровадження штучного інтелекту в обороноздатність держави.

У загальній архітектурі освітньо-науковий блок виконує функції на трьох

рівнях: військово-педагогічна система, цивільно-академічна інтеграція та кваліфікаційна підготовка та допідготовка.

До військово-педагогічної системи належать Національний університет оборони України [55], інші вищі військові навчальні заклади. Національний університет оборони України здійснює оперативно-стратегічну підготовку військово-політичного керівництва, кадрів C4ISR та ситуаційного аналізу. C4ISR – це інтегрована військова концепція та мережа систем, яка розшифровується як Command (C1), Control (C2), Communications (C3), Computers (C4), Intelligence (I), Surveillance (S), and Reconnaissance (R): командування, управління, зв'язок, комп'ютери, розвідка, спостереження та рекогностування (рис. 2.4).

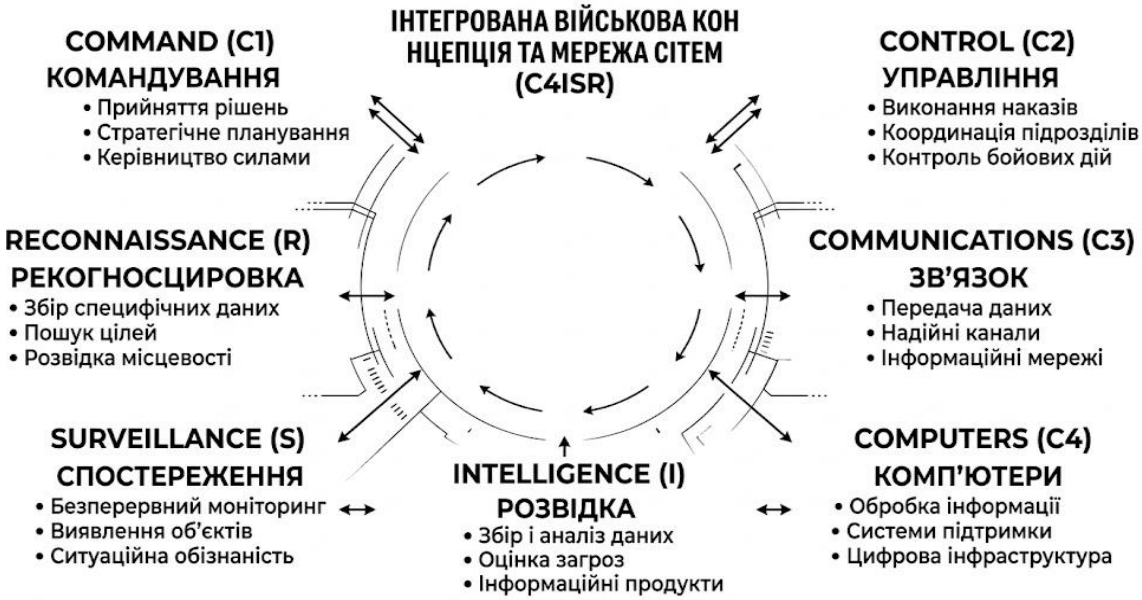

Рис. 2.4. Схема C4ISR

Джерело: створено автором на основі [63]

Вона здійснює координацію дій між військовими, поєднуючи дані з дронів, супутників і датчиків у реальному часі для швидкого ухвалення рішень [13; 63]. Функція командування акумулює повноваження та відповідальність за планування й управління силами, забезпечуючи цифрову підтримку ухвалення рішень, доведення наказів і керівництво підрозділами. Управління реалізується через моніторинг виконання завдань, контроль проходження наказів та фіксацію

відхилень для корекції рішень командира. Зв'язок гарантує передавання даних від солдата до вищого військово-політичного керівництва на основі сучасних протоколів та інструментів планування. Комп'ютерні системи слугують апаратно-програмним базисом обробки й зберігання інформації. Своєю чергою, розвідка формує єдину інформаційну картину оператора, спостереження забезпечує неперервний моніторинг простору за допомогою керованих програмним забезпеченням датчиків (камер, раддарів, БпЛА) із функцією автоматичного оповіщення, а рекогносцировка орієнтована на цілеспрямований збір інформації за конкретними запитами [63].

Вищі військові навчальні заклади готують фахівців із кіберзахисту, безпілотних систем, програмування ШІ-моделей та експлуатації цифрових комплексів. Такими закладами є Військовий інститут телекомунікацій та інформатизації імені Героїв Крут [19], Харківський національний університет Повітряних Сил імені Івана Кожедуба [151], Військова академія м. Одеса [18] та інші.

Цивільно-академічна інтеграція означає впровадження спільних освітніх та дослідно-конструкторських програм цивільних університетів з Міноборони та Brave1 для розробки ШІ-алгоритмів, обробки великих даних (Big Data) та комп'ютерного зору. Дослідно-конструкторські та науково-дослідні програми у сфері штучного інтелекту в цивільних університетах України активно розвиваються через роботу спеціалізованих кафедр, лабораторій та партнерство з ІТ-бізнесом і міжнародними консорціумами. Наприклад, на базі Навчально-наукового інституту прикладного системного аналізу НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» діє профільна Кафедра штучного інтелекту [58]. Ключовою розробкою кафедри є створення систем інтелектуальної обробки даних, нових методів розпізнавання та обробки графічних зображень і текстових документів. У межах наукової школи обчислювального інтелекту ведуться конструкторські дослідження щодо побудови діагностичних систем.

Мінцифри розробило каталог освітніх програм для вступників

університетів з інформацією про підготовку фахівців у галузі штучного інтелекту. В каталозі – аналіз даних, машинне навчання, комп'ютерний зір, розпізнавання образів, обробка природної мови [15].

Фундаментальною основою практичної стійкості та бойової ефективності інституційної архітектури впровадження ШІ є скрізна функція кваліфікаційної підготовки та допідготовки. Вона забезпечує безперервний цикл перетворення науково-технічних розробок і проєктів на операційні спроможності безпосередньо для підрозділів Сил оборони. Ця функція охоплює такі критичні напрями: спеціалізована перепідготовка операторів прикладних ШІ-платформ; підготовка фахівців із роботизованих та безпілотних систем; спеціальна підготовка фахівців із РЕБ/РЕР у контексті ШІ; управління життєвим циклом компетенцій. Кваліфікаційна підготовка реалізується через мережу спеціалізованих навчальних центрів ЗСУ, сертифікованих тренінгових програм, спільних курсів із розробниками (Defense AI Center «A1») та програм підвищення кваліфікації на базі вищих військових навчальних закладів.

На основі вищезазначеного, вважаємо за потрібне уточнити запропоновану на рис. 2.3. інституційну архітектуру забезпечення ШІ у сфері обороноздатності України, додавши освітньо-науковий блок (Рис. 2.5).

Рис. 2.5. Інституційна архітектура забезпечення ШІ у сфері обороноздатності України

Джерело: створено автором на основі аналізу нормативно-правових актів

Воєнний стан розширює компетенцію органів державної влади [101], тоді як необхідність швидко реагувати на загрози стимулює «експериментальне» впровадження інновацій [170]. Водночас у міру стрімкого накопичення практики зростає небезпека її відхилення від правових норм: відсутність чітких правил підвищує ймовірність помилок, судових і дипломатичних наслідків, а також ускладнює співпрацю з партнерами, які очікують дотримання власних етичних та правових стандартів [130]. Тому державна політика має не обмежувати розвиток, а забезпечувати створення гнучких, але водночас передбачуваних процедур, спроможних діяти й після завершення воєнного стану.

Аналізуючи інституційну складову публічного управління, повноваження суб'єктів та їх функціональну взаємодію у процесі використання штучного інтелекту в підвищенні обороноздатності України, варто звернути увагу на наступні аспекти управлінської діяльності. Встановлено, що інституційна архітектура регулювання використання ШІ є недостатньо скоординованою та узгодженою. Пропонується створити міжвідомчий координаційний центр за участю Міністерства оборони, Генерального штабу, Мінцифри та інших уповноважених суб'єктів, який буде відповідати за формування узгодженої політики у сфері обороноздатного ШІ. Також варто продовжувати посилювати міжнародне співробітництво з державами-партнерами, демонструвати практики використання ШІ та долучатися до роботи багатосторонніх форумів з метою демонстрації зростання обороноздатності, підвищення впливовості держави на міжнародній арені, покращення її іміджу серед світової спільноти. Подальший розвиток державної політики у сфері оборонного штучного інтелекту потребує інституціоналізації комплексної системи публічного управління, орієнтованої на стратегічне планування, міжвідомчу координацію, кадрову й наукову підтримку інновацій, активізацію державно-приватного співробітництва та досягнення взаємосумісності з європейським і євроатлантичним безпековим простором [117].

І обов'язковими заходами для покращення та вдосконалення інституційних засад впровадження штучного інтелекту в секторі безпеки і

оборони України повинні стати заходи з забезпечення належного рівня підготовки персоналу: організація навчання для командирів, операторів і юристів, уповноважених здійснювати правовий огляд та оцінювати використання ШІ, підвищення кваліфікації представників публічного управління.

2.3. Інтеграція ШІ-рішень у процеси управлінської діяльності як чинник підвищення обороноздатності України

Сфера управління за своєю сутністю є складною, багатоаспектною та динамічною категорією. У загальнонауковому розумінні управління постає як діяльність уповноважених органів, спрямована на досягнення конкретних завдань за допомогою відповідних методів, форм, способів і функцій [25]. Класичні підходи наголошують на здатності управління перетворювати розрізнені ресурси та людський потенціал на ефективно організовану, цілеспрямовану та продуктивну систему [179].

У системі державних функцій особливе місце посідає управлінська діяльність у сфері обороноздатності, яка визначається як цілеспрямований процес формування, розвитку та використання військово-політичного, економічного й соціального потенціалу держави для захисту її суверенітету від зовнішньої агресії. Ця діяльність базується на принципах цивільно-військового співробітництва, стратегічного планування та сучасних світових стандартах публічного адміністрування.

Фундаментальною основою зазначеної діяльності є поняття «обороноздатність». Закон «Про оборону України» визначає її як «здатність держави до захисту у разі збройної агресії або збройного конфлікту» [97]. При цьому обороноздатність складається з матеріальних і духовних елементів та є сукупністю воєнного, економічного, соціального та морально-політичного потенціалу у сфері оборони й належних умов для його реалізації [97]. Вона безпосередньо пов’язана зі станом і структурою збройних сил держави, їхнім

бойовим потенціалом, рівнем підготовки особового складу та бойової готовності військ, рівнем технічного оснащення та логістичного забезпечення [61]. Як зазначає М. Хавронюк, стан обороноздатності відображають мобілізаційні можливості держави, кількість і якість її Збройних Сил, їхня здатність оперативно переходити на воєнний стан та організовано виконувати завдання з відсічі агресії [54].

Поняття «обороноздатності» стало особливо актуальним під час широкомасштабної збройної агресії росії проти України. Традиційно обороноздатність визначається як здатність держави до безпосередньої військової відсічі агресії. Проте ціннісний підхід до розуміння обороноздатності наголошує на тому, що обороноздатність – це здатність держави захищати власні суверенні та національні цінності: права, свободи, безпеку та незалежність. Таке розуміння варто підсилити концептом оборони цивілізаційних цінностей – гуманізму, миру, верховенства права та демократичних свобод тощо. Ця війна не є лише територіальним конфліктом. Він має виразний цивілізаційний характер, де відбувається екзистенційне протистояння між авторитаризмом та демократичним світом, між варварством та гуманізмом, добром і злом. Поглиблюючи цей підхід, Л. Демидова виокремлює в структурі обороноздатності ключові складові: 1) захист цінностей (прав, свобод людини та інтересів суспільства і держави), що є важливими для держави та суспільства; 2) спроможність держави до захисту від воєнних та і інших суттєвих шкідливих небезпек; 3) превентивна спроможність держави культурного, виховного, політичного, правового, навчального, мобілізаційного характеру [28].

Збройна агресія рф проти України та запровадження правового режиму воєнного стану зумовили трансформацію цілей державного управління, що змінює саму його парадигму. У мирний період ефективність державного управління визначається рівнем соціально-економічного розвитку, підвищенням якості публічних послуг, стабільністю правопорядку та реалізацію прав і свобод людини. Війна радикально змінила ієрархію управлінських цілей. Відбувся системний перехід від парадигми «управління розвитком» до парадигми

«забезпечення існування», де головними критеріями ефективності стають інституційна спроможність, збереження суверенітету й територіальної цілісності в умовах екзистенційних загроз. Пріоритетними завданнями стала оборона держави, забезпечення відсічі агресору, мобілізація ресурсів, підтримання керованості та забезпечення безперервності функціонування державних інституцій. Усі напрями діяльності державних органів підпорядковуються необхідності забезпечення та зміцнення обороноздатності держави.

У сучасній науковій інтерпретації Л. Перевалової, О. Кузьменко та Я. Григоренка обороноздатність держави постає як комплексна характеристика рівня підготовленості її економіки, населення та збройних сил до нейтралізації зовнішньої агресії, забезпечення територіальної цілісності та збереження державної незалежності [61]. Вона формується під впливом характеру реальних і потенційних воєнних загроз; участі держави в міжнародних структурах колективної безпеки та оборонного співробітництва; рівня розвитку воєнного потенціалу; наявних матеріальних, духовних, економічних, науково-технічних ресурсів і людського капіталу; ступеня соціальної та міжетнічної згуртованості суспільства; морально-психологічної готовності громадян до захисту держави; а також ефективності державного й воєнного управління [61].

У сучасних умовах значення управлінської діяльності критично зростає, першочергово у сфері забезпечення обороноздатності [115; 116]. Оскільки Україна перебуває у стані війни, це зумовлює актуалізацію всього спектра безпекових викликів, які формують предметне поле обороноздатності держави. Українські науковці розглядають управління як інтегративний процес, що охоплює планування, організацію, мотивацію та контроль [145]. Класичними компонентами управлінського процесу є прогнозування, планування, програмування, організація, регулювання, координація та контроль [152]. Причому у теорії публічного управління ці елементи складають послідовний управлінський цикл (Рис. 2.6), а також розглядаються як взаємопов’язані та безперервні функції, що в умовах воєнного стану вимагають максимальної інтеграції, динамічності та адаптивності. Кожний із цих складників відіграє

важливу роль у досягненні стратегічних цілей, найголовнішою із яких є забезпечення обороноздатності.

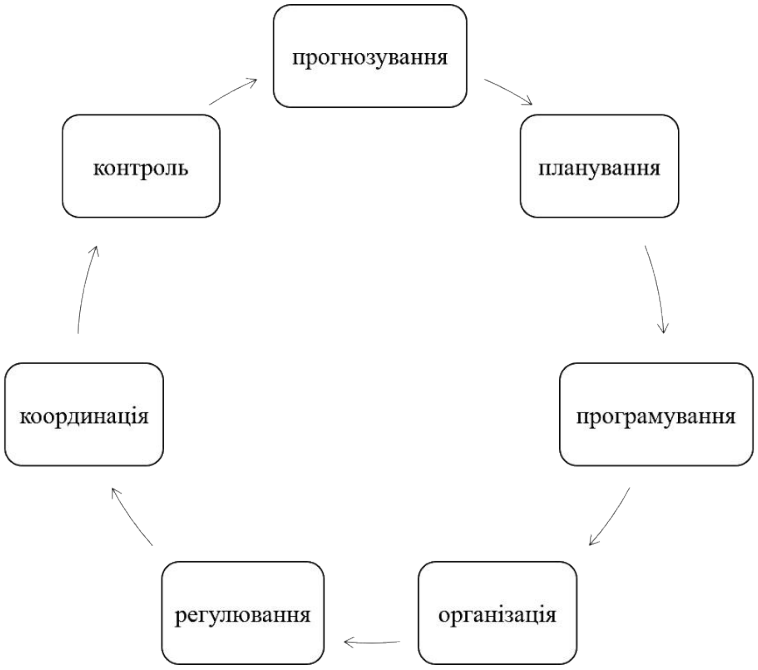

Рис. 2.6. Етапи управлінського циклу

Джерело: створено автором на основі [152]

Зазначені елементи (рис. 2.6) є послідовними етапами єдиного управлінського циклу, де вихідне прогнозування формує аналітичну основу для планування, яке деталізується через програмування або ресурсне забезпечення. Реалізація розроблених програм вимагає етапу організації, що в процесі виконання коригується шляхом регулювання та узгоджується через координацію. Завершальним елементом управлінського циклу є контроль. Саме він генерує зворотний зв'язок, який стає підґрунтям для нового прогнозування.

У системі функцій публічного адміністрування прогнозування посідає вихідне, базове місце, оскільки саме воно формує аналітично-інформаційне підґрунтя для всіх наступних етапів управлінського циклу – від планування та програмування до організації й підсумкового контролю. Особливого значення прогнозування набуває в умовах масштабних суспільних трансформацій та системних криз. Публічне управління в таких умовах повинне не просто реагувати на виклики, а передбачати їх, формувати випереджальні рішення для

забезпечення сталого розвитку у довгостроковій перспективі [32]. Під час війни прогнозування набуває стратегічного значення для національної обороноздатності, оскільки потрібно передбачати ймовірні загрози, дії агресора, оцінювати міцність критичної інфраструктури та ресурсну спроможність держави.

Планування є підґрунтям управлінського процесу, адже передбачає визначення цілей, розроблення стратегій і прогнозування можливих сценаріїв розвитку. Воно дає змогу передбачати виклики, оптимізувати ресурси і створювати чіткі орієнтири для діяльності. Ефективне планування потребує аналізу внутрішніх і зовнішніх чинників, що впливають на процес, а також гнучкості для коригування планів у відповідь на нові обставини [145].

У сучасному управлінні планування набуває особливої ваги через швидкі зміни у технологіях та умовах, в яких воно відбувається. За аналогією з управлінням підприємствами, у кризових періодах, яким, зокрема, є війна, публічне управління повинне набувати нових системних якостей: гнучкості, адаптивності, високої швидкості реагування на виклики та спроможності до оперативної переорієнтації діяльності. В ситуаціях невизначеності, які пов’язані, зокрема, з інтенсивними обстрілами, руйнуванням інфраструктури, блекаутами, порушенням логістики, скорочуються терміни планування. Довгострокові стратегії поступаються місцем адаптивному інструментарію, який потребує постійного коригування відповідно до умов, що динамічно змінюються. Тому планування перетворюється на робочий інструмент, який можна і потрібно оперативно переглядати відповідно до обставин, які змінюються. Публічне управління має володіти інструментом сценарного планування, тобто мати декілька варіантів розвитку подій: позитивний – коли ситуація керована та їй не загрожують певні виклики; базовий та кризовий. Для кожного такого «сценарію» повинен бути готовий план дій, який повинен бути детальним і чіткім. Ще одна вимога до планування в умовах війни – мати уявлення про наявні та потенційні ресурси, що можуть бути задіяні в тій або іншій ситуації. Також повинні бути резервні ресурси на випадок пошкодження складів, систем управління, логістики

тощо. Функція планування має охоплювати всі рівні публічної влади, забезпечуючи принцип інституційної взаємозамінності: у разі дезорганізації центральних органів управлінські функції та відповідальність за критичні процеси мають оперативно перебирати органи нижчого рівня.

Програмування виступає сполучною ланкою між стратегічним баченням проблеми та її практичною реалізацією. Програмування визначає ресурси, часові рамки, цільові програми, індикатори ефективності досягнення поставленої мети, встановлює «правила гри». В умовах воєнного стану традиційне державне програмування також трансформується. Відбувається перехід від довгострокових бюджетних програм до гнучких цільових ініціатив швидкого реагування. Прикладом є державні грантові програми для оборонних технологій, розвиток кластерів на кшталт Brave1 тощо. На етапі програмування публічне управління повинне враховувати також міжнародну технічну допомогу, логістичні ланцюжки постачання західного озброєння та спільні оборонні проєкти з партнерами.

Організація – це складова частина управлінського процесу, яка забезпечує створення структури для практичної реалізації розроблених планів і стратегій. Вона охоплює раціональний розподіл ресурсів, делегування повноважень, координацію діяльності підрозділів і встановлення комунікаційних каналів [145]. На сучасному етапі функція організації зазнає суттєвої трансформації: жорсткі бюрократичні й вертикально-ієрархічні структури поступаються місцем гнучким матричним, мережевим та командним підходам. У контексті забезпечення обороноздатності та функціонування публічної влади в умовах війни така гнучкість стає вирішальним чинником стійкості, оскільки дає змогу інституціям оперативно реагувати на критичні зміни, мінімізувати бюрократичні затримки та підвищувати ефективність міжвідомчої взаємодії.

Регулювання – це функція публічного управління, спрямована на усунення відхилень від накресленого курсу, нейтралізацію дестабілізуючих чинників і підтримку стійкості системи в умовах динамічного середовища. Регулювання забезпечує динамічну гнучкість управління у разі виникнення незапланованих

внутрішніх чи зовнішніх зсувів. Ця гнучкість виявляється, наприклад, в усуненні бюрократичних бар'єрів для прискорення прийняття важливих рішень. В умовах війни регулювання здійснюється в режимі реального часу: органам публічного управління доводиться оперативно реагувати на обстріли, руйнування критичної інфраструктури, зміни на лінії фронту чи блекаути.

З регулюванням тісно пов'язана координація. Якщо регулювання визначає, що і як потрібно змінити в ході процесу, то координація забезпечує, щоб усі учасники системи зробили це узгоджено та одночасно. Іншими словами, координація – це інтеграційний механізм, який дозволяє узгодити, синхронізувати та гармонізувати діяльність всіх суб'єктів публічного управління для досягнення єдиної стратегічної мети та забезпечення синергетичного ефекту їхньої діяльності. Це дозволяє здолати міжвідомчу роз'єднаність або ізольованість різних інституцій. В ідеалі координація сприяє запобіганню дублюванню функцій між різними міністерствами та відомствами. В умовах війни на цьому етапі відбувається синхронізація дій військового командування, органів виконавчої влади, місцевого самоврядування, волонтерського сектору та приватного бізнесу для досягнення певної мети. З іншого боку, відбувається координація оборонних потреб із матеріально-технічними, фінансовими та інформаційними ресурсами міжнародних партнерів. Недостатня координація між центральними органами, військовими структурами та місцевим самоврядуванням може призвести до конфліктів при прийнятті рішень або затримок у їх виконанні, можуть бути прийняті рішення без урахування конкретної ситуації на місцях, що послаблює оперативність реагування й підриває довіру до управлінських інституцій [48].

Контроль є однією з основних функцій управління та завершальною стадією циклу всього процесу управління. Одночасно ця складова процесу управління виступає рушійною силою початку нового циклу управління. Контроль передбачає отримання актуальної інформації про стан справ, забезпечує своєчасність виявлення порушень і реагування на них для подальшої ефективної роботи органу, установи чи окремого департаменту тощо [152]. У

сучасному публічному управлінні контроль набуває багатогранного характеру. Його здійснюють традиційними – фінансовий або операційний контроль, або інноваційними методами. Контроль дає можливість своєчасно виявляти відхилення від запланованих цілей, коригувати дії та забезпечувати відповідність результатів стратегічним пріоритетам [152]. На етапі контролю визначаються критерії, здійснюється перевірка та встановлюються результати діяльності та запроваджуються корективи, якщо результат суттєво відрізняється від запланованого, або не відповідає критеріям [152]. Особливістю контролю у сфері державного управління є його безперервність, тобто протягом усього процесу управління, починаючи з планування й до досягнення поставлених цілей [152]. Метою контролю у публічному управлінні є недопущення відхилень від запланованих норм та усунення негативних наслідків у разі їх виявлення задля досягнення поставлених цілей [152]. Контроль в публічному управлінні також необхідний задля дотримання дисципліни та порядку, він забезпечує чіткість та конкретність прийнятих рішень.

Розглянувши етапи процесу публічного управління можемо узагальнити та уточнити зміст діяльності та визначити його специфіку в умовах воєнного стану (Табл. 2.6).

Таблиця 2.6

Специфіка публічного управління в умовах воєнного стану

Етап	Компонент	Зміст діяльності в публічному управлінні	Специфіка в умовах воєнного стану
1	Прогнозування	Аналіз тенденцій, бачення майбутнього стану, визначення ймовірних загроз та альтернативних сценаріїв	Моделювання дій ворога, використання ситуаційної аналітики та прогнозування потреб фронту або тилу
2	Планування	Формулювання стратегічних і тактичних цілей, вибір оптимального сценарію дій, формування «правил гри».	Перехід до короткострокового, адаптивного та сценарного планування.
3	Програмування	Трансформація планів у конкретні цільові програми із закріпленням часових рамок та ресурсів.	Розробка цільових оборонних та матеріально-технічних програм, розрахунок резервів і критичних ресурсів.

Продовження таблиці 2.6

Етап	Компонент	Зміст діяльності в публічному управлінні	Специфіка в умовах воєнного стану
4	Організація	Формування управлінської структури, розподіл повноважень, завдань та відповідальності.	Відхід від жорсткої бюрократичної вертикалі до гнучких, матричних та командно-мережевих структур.
5	Регулювання	Усунення відхилень від накресленого курсу, оперативне реагування на незаплановані зміни.	Негайне реагування на форс-мажори (обстріли, руйнування логістики, блекаути) у режимі реального часу.
6	Координація	Узгодження дій усіх суб'єктів управління для досягнення синергетичного ефекту.	Забезпечення цивільно-військового співробітництва, міжвідомчої взаємодії та комунікації між інституціями.
7	Контроль	Перевірка відповідності фактичних результатів запланованим, виявлення системних помилок.	Безперервний аудит використання ресурсів, перевірка готовності оборонних систем та бойової здатності.

Джерело: створено автором

В умовах воєнного стану межі між цими етапами розмиваються, перетворюючи управлінську діяльність на цілісний, високооперативний і безперервний процес, у ході якого відбувається комплексна реалізація взаємопов'язаних функцій державного управління. Виконання цих функцій формує комплексний механізм публічного управління розвитком і використанням штучного інтелекту у сфері оборони, вибудовуючи сучасну модель державного управління, яка ґрунтується на стратегічному плануванні, міжвідомчій координації, цифровій трансформації, розвиткові людського потенціалу та відповідальному використанні інноваційних технологій. Це посилить обороноздатність України, зміцнить національну безпеку та забезпечить технологічну переваги держави в умовах сучасних воєнних викликів [118.

Українські дослідники звертають увагу на ще один аспект публічного управління. Так, В. Торічний та І. Максимів вважають, що рушійною силою активізації людського потенціалу у публічному управління виступає мотивація. Її слід розглядати як особливий компонент управління, який спонукає

працівників досягати організаційних цілей через задоволення їхніх особистих потреб [145]. Такими потребами може бути фінансова задоволеність, визнання, можливості професійного зростання тощо. Управлінська діяльність у сфері безпеки й оборони потребує високого рівня професіоналізму, дисципліни та відданості, що неможливо забезпечити без ефективної системи мотивації, – роблять висновок автори статті [145]. У контексті триваючої повномасштабної збройної агресії російської федерації високий рівень мотивації публічних службовців є критично важливим для безперервності державного управління, збереження керованості держави та забезпечення її інституційної стійкості [144]. Підставою для таких висновків є теорія мотивації публічної служби (PSM) [206; 224], яка пояснює готовність діяти в інтересах суспільства навіть за відсутності еквівалентних приватних вигод. Висока внутрішня мотивація до публічної служби (патріотизм, усвідомлення важливості своєї роботи для перемоги та безпеки) гарантує безперервність функціонування органів державної влади та спонукає до підсилення обороноздатності країни, про що свідчать дослідження [2; 3]. Зокрема, І. Куцій [45] зазначає низку особливостей, що відрізняють мотиваційне середовище вітчизняної держслужби від загальнотеоретичних моделей. По-перше, під час воєнного стану сформувався унікальний мотиваційний контекст вітчизняних держслужбовців – збройна агресія стала чинником, що спонукає до якіснішої та інтенсивнішої роботи; по-друге, кар'єрний успіх асоціюється у них з тріадою «велика зарплата – велика відповідальність – великі можливості для країни», що свідчить про органічне поєднання матеріальних і патріотичних мотивів.

Отже, аналіз наукової літератури та сучасних реалій дозволив зробити висновок про те, що в умовах воєнного стану публічне управління модернізується, трансформується, стає більш адаптивним та гнучким, обираючи нетрадиційні методи та способи. Висока внутрішня мотивація до публічної служби сприяє підвищенню обороноздатності держави.

Обороноздатність посилюється і завдяки розвиткові цифровізації. Так, Дослідження організаційної культури публічної служби (2023) показало, що

84,7% службовців зазначили, що цифровізація дозволяє працювати їм ефективніше [2]; за даними опитування 2025 року, ця частка зросла до 87,5% [3].

Така позитивна динаміка сприйняття цифрових інструментів створює сприятливе підґрунтя для широкої інтеграції технологій штучного інтелекту в публічне управління оборонним сектором. За аналітичними висновками Stanford AI Index 2025, тема штучного інтелекту вийшла за межі технологічної дискусії та безпосередньо стосується якості державного управління, а саме: якості державних рішень, швидкості реагування на виклики, довіри громадян і здатності публічної служби бути сучасною [17]. Як зазначає В. Василенко, використання ШІ-систем у сфері державного управління створює якісно нове середовище, у якому цифрові технології отримують доступ до критичних процесів, що безпосередньо впливають на загальнодержавну безпеку та рівень обороноздатності країни [16]. Впровадження інноваційних алгоритмів ШІ стає вирішальним фактором підвищення обороноздатності держави, спроможним суттєво трансформувати її стратегічний ресурс та змінювати баланс сил на міжнародній арені [21].

Тому перед суб'єктами публічного управління постає стратегічне завдання – розробити адаптивні механізми регулювання, контролю та координації процесу інтеграції штучного інтелекту для забезпечення національної безпеки та зміцнення могутності держави [21]. Використання штучного інтелекту в оборонній сфері вимагає від публічних інституцій гнучкого, випереджального й цілісного управлінського впливу. Водночас класичні бюрократичні моделі, орієнтовані на покрокові й тривалі процедури, виявляють свою неспроможність у реаліях алгоритмізованої агресії, інтенсивного використання безпілотних систем та необхідності опрацювання великих масивів даних (Big Data) у режимі реального часу [21].

Для забезпечення ефективного державного регулювання процесів розробки та впровадження штучного інтелекту в оборонній сфері О. Вольська пропонує чотири групи публічно-управлінського інструментарію: нормативно-регуляторний, інституційно-організаційний, інформаційно-аналітичний та

кадрово-інвестиційний [21].

На противагу цьому, у дисертаційному дослідженні зауважено, що інтеграцію ШІ-рішень задля підвищення обороноздатності України доцільно аналізувати крізь призму цілісного управлінського циклу: прогнозування, планування, програмування, організації, регулювання, координації та контролю. Такий підхід спирається на розуміння штучного інтелекту як комплексу алгоритмів і моделей, спроможних здійснювати аналіз, прогнозування, класифікацію та формувати рішення, що раніше належали до виключної компетенції людини [16]. Отже, його послідовне залучення на всіх етапах публічного управління виступає об'єктивно зумовленим кроком. По-друге, зазначені етапи формують єдину циклічну систему, де кожен елемент взаємопов'язаний із наступним та реагує на виклики зовнішнього середовища. В екстремальних умовах воєнного стану чіткі межі між цими стадіями трансформуються, гарантуючи управлінському процесу адаптивність, високу оперативність та безперервність.

На етапі прогнозування штучний інтелект виступає синергетичним механізмом інтелектуального аналізу даних, предиктивного моніторингу та ситуаційного моделювання. Алгоритмам ШІ делегуються функції оперативного виявлення загроз [21], кібераналітики й автоматизованого реагування на інциденти [1]. У цьому контексті органи публічного управління, дотичні до сфери обороноздатності, застосовують ШІ для виявлення поведінкових аномалій у державних і військових мережах, прогнозування напрямів складних небезпек та їхньої миттєвої локалізації. Це дозволяє зменшити ланцюжок бюрократичного погодження та прийняття управлінських рішень. Крім того, ШІ-технології забезпечують високу точність під час моделювання військових операцій, прогнозування сценаріїв розвитку подій та оцінювання їхніх потенційних наслідків. Загалом трансформація функції прогнозування в сучасному публічному управлінні відбувається за кількома ключовими напрямами. По-перше, інерційне прогнозування повністю замінюється сценарним, у межах якого минулий досвід, поточна ситуація, зовнішні чинники та інші масиви даних

комплексно аналізуються ШІ-системами, що дозволяє розробити декілька альтернативних сценаріїв розвитку подій. Такими сценаріями розвитку можуть стати оптимістичний, базовий або кризовий. ШІ допомагає розглянути деталі таких сценаріїв, використовуючи аналітичні платформи, засоби розвідки на основі відкритих джерел (OSINT) та моделі машинного навчання для автоматизованого виявлення «слабких сигналів» загрози, випереджального аналізу та оптимізації управлінських рішень у режимі реального часу. Тобто розпізнавання слабких сигналів стає другим напрямом трансформації функції прогнозування, оскільки перетворюється зі статичного аналітичного етапу на динамічну, цифровізовану та адаптивну систему, яка забезпечує інституційну стійкість держави перед обличчям глобальних та воєнних викликів. Наочними прикладами такого використання ШІ у процесі публічного управління є вітчизняна ШІ-платформа «SPECTR», яка дозволяє прогнозувати ймовірні кроки противника [52], а також система на базі SAP, яка суттєво підвищує прогнозованість і прозорість логістичних процесів у Силах оборони України [146].

На етапі планування використання ШІ-технологій у публічному управлінні прискорює прийняття критично важливих рішень і безпосередньо підвищує обороноздатність держави в умовах воєнного стану. Інтеграція систем підтримки прийняття рішень (Decision Support Systems – DSS) на основі алгоритмів штучного інтелекту трансформує процес публічного управління оборонним сектором, забезпечуючи високу оперативність, обґрунтованість та предиктивний характер управлінських впливів в умовах високого рівня невизначеності. Системи підтримки прийняття рішень – інтелектуальні комп’ютерні системи, які шляхом аналізу великих масивів даних (Big Data), моделювання сценаріїв та застосування алгоритмів машинного навчання допомагають керівникам (як цивільним публічним службовцям, так і військовому командуванню) приймати обґрунтовані, оперативні та зважені рішення. Автоматизований моніторинг та аналіз глобального медіаполя, виявлення в режимі реального часу ворожих інформаційно-психологічних операцій, маніпулятивних кампаній та

деструктивного контенту, включно з дипфейками, який здіснюють ШІ-системи, забезпечують прийняття виважених та скоординованих рішень, які передбачають ефективні результати [26]. ШІ-системи здатні виконувати семіотичний аналіз та обробляти розвідувальні дані у режимі реального часу, що скорочує час від виявлення загрози до прийняття рішення, надаючи командуванню та органам публічної влади сформовані варіанти дій або рішення. При плануванні операцій використовується ШІ-система SPECTR, яка на основі унікального масиву даних перетворює їх на реальну перевагу на полі бою. Система аналізує інформацію, виявляє закономірності, формує рекомендації для планування операцій і організації процесів у війську [52]. Отже, використання ШІ-технологій дозволяє публічному управління перейти до принципів стратегічного та оперативно-тактичного планування.

На етапі програмування публічного управління у сфері обороноздатності застосування технологій штучного інтелекту забезпечує якісний перехід від статично-бюрократичного до динамічного та ресурсно-оптимізованого формування державних цільових програм. На етапі програмування технології штучного інтелекту забезпечують виконання низки взаємопов'язаних завдань, серед яких автоматизована декомпозиція та структуризація стратегічних цілей, усунення внутрішніх суперечностей оборонних програм, ресурсне та бюджетне програмування тощо. За допомогою алгоритмічних трансляторів, зокрема сучасних NLP/LLM-моделей, ШІ-інструменти аналізують базові стратегічні документи, автоматично формуючи розгалужене дерево цілей і завдань для конкретних державних оборонних програм. Водночас спеціальні алгоритми здійснюють перевірку проєктів на предмет дублювання заходів, конфліктів міжвідомчих завдань та відсутності нормативного забезпечення, що дозволяє мінімізувати внутрішні суперечності. У випадку ресурсного та бюджетного програмування методи машинного навчання застосовуються, наприклад, для розподілу ресурсів у випадку, коли органу публічного управління потрібно врегулювати питання співвідношення коштів для розвитку безпілотних систем і закупівлі традиційної бронетехніки задля досягнення максимального

оборонного ефекту. Завдяки розрахунку вартості життєвого циклу штучний інтелект моделює повну вартість розробки, закупівлі, експлуатації, обслуговування та утилізації засобів озброєння та військової техніки, запобігаючи закладанню в програми недофінансованих проєктів. В умовах високоінтенсивної війни критично важливим є формування гнучких оборонних програм та проєктного управління. Штучний інтелект вивчає та аналізує зміни у характеристиках загроз і фронтовій ситуації, пропонуючи оперативні корективи до строків, обсягів закупівель і технічних вимог без перегляду всієї стратегії. Одночасно інтелектуальний аналіз даних забезпечує пріоритетизацію DeepTech-проєктів через оцінку рівня їхньої технологічної зрілості. Завершується цей процес комплексним моделюванням та оцінкою ризиків виконання програм, у межах якого ШІ здійснює сценарний аналіз ланцюгів постачання елементної бази (мікросхем, рідкісних металів, компонентів) для прогнозування логістичних збоїв, а також оцінює виробничі потужності, фінансову стійкість і кадрову забезпеченість підприємств оборонно-промислового комплексу перед їх затвердженням як головних виконавців цільових програм.

На етапі організації у сфері обороноздатності застосування інструментів штучного інтелекту забезпечує системну трансформацію традиційних ієрархічних структур у гнучкі, мережево-центричні системи, оптимізуючи інституційну та організаційно-штатну архітектуру суб'єктів управління. Алгоритмічний аналіз нормативно-правових актів, регламентів і посадових інструкцій дозволяє виявляти та усувати застарілі або дубльовані функції, а на основі аналізу інтенсивності інформаційних потоків і поточного навантаження – здійснювати моделювання крос-функціональних команд та міжвідомчих ситуаційних центрів під конкретні воєнно-технологічні завдання. ШІ-системи використовуються також для перехоплення швидкісних цілей, як-от реактивних дронів чи крилатих ракет – система здатна миттєво обробляти траєкторію польоту, одночасно враховуючи зовнішні фактори: силу вітру, вологість, температуру та висоту для точного керування засобом ураження, зо дозволяє організувати швидкий захист та забезпечити оборону критичних об'єктів [117].

У межах інтелектуального управління людськими ресурсами ШІ-технології забезпечують автоматизовану оцінку компетенцій фахівців у сфері публічного адміністрування та ІТ, створення динамічних карт спеціальностей для формування висококваліфікованих підрозділів аналітики та цифровізації, а також моніторинг показників професійного вигорання персоналу в умовах воєнного стану задля збереження кадрового потенціалу.

Особливого значення набуває напрям AI-орієнтованої оборонної логістики, де алгоритми здійснюють автоматичний розрахунок і динамічне проектування маршрутів постачання озброєння, боєприпасів, пального та медичного майна з урахуванням логістичних ризиків і дій ворога, а також реалізують концепцію предиктивного обслуговування оборонної техніки на основі аналізу зносу її компонентів. Зокрема, на цьому етапі використовують можливості SAP – світового стандарту у сфері управління ресурсами, який використовують понад 90% армій країн НАТО. Це дозволяє об'єднати дані з різних напрямів забезпечення в єдиній системі, забезпечити їхню актуальність і підтримати ухвалення рішень на основі достовірної аналітики. Система SAP дозволяє бачити фактичну наявність ресурсів у режимі реального часу; відстежувати їхній рух між підрозділами; планувати постачання та закупівлі; контролювати фінансові операції та витрати [120]; підвищувати керованість логістичних процесів [146].

Нарешті, на етапі організації штучний інтелект відіграє вирішальну роль у формуванні єдиного безпекового дата-центричного середовища: алгоритми здійснюють структурування та автоматичну класифікацію різнорідних великих масивів даних (Big Data), що надходять від цивільних і військових органів влади, долаючи прояви відомчої ізольованості та забезпечуючи алгоритмічний контроль за рівнями доступу до конфіденційної та військової інформації у режимі реального часу.

На етапі регулювання застосування штучного інтелекту передбачає перехід від жорсткого нормативного консерватизму до випереджального та адаптивного регулювання, здатного оперативно реагувати на появу новітніх

технологій і непередбачувані виклики воєнного середовища. Крім того, випереджальне регулювання дозволяє виявляти відхилення й ризики ще до їх фактичного настання та пропонувати алгоритми їх негайної нейтралізації [21]. Важливим аспектом є розробка гнучких регуляторних механізмів на кшталт «регуляторних пісочниць» та підходів soft law, які дозволяють швидко тестувати, кодифікувати й інтегрувати інноваційні рішення, розроблені в межах платформи Brave1, без очікування тривалих циклів внесення змін до законів.

Водночас регуляторний процес охоплює створення систем технічного нормування і стандартизації, які гарантують сумісність, стійкість до кібератак та захист критичних даних алгоритмів. Окрему увагу на цьому етапі зосереджено на встановленні чітких нормативних гарантій та етичних обмежень щодо застосування штучного інтелекту в системах підтримки прийняття рішень, зокрема законодавчого закріплення принципу обов'язкової участі людини у критичних контурах ухвалення рішень, що дозволяє мінімізувати алгоритмічні похибки та забезпечити дотримання норм міжнародного гуманітарного права під час ведення оборонних дій.

Етап координації виступає головним чинником подолання відомчої ізольованості та забезпечення мережево-центричної узгодженості дій усіх суб'єктів обороноздатності. Завдяки реалізації концепції наскрізного обміну даними та обробці мультидоменних масивів інформації у режимі реального часу, ШІ-алгоритми забезпечують горизонтальну інтеграцію між цивільними технологічними відомствами, оборонно-промисловим комплексом, інноваційними платформами та безпосередньо військовим командуванням. Це дозволяє суттєво скоротити часові інтервали між формуванням оперативної потреби на фронті та її технологічним забезпеченням, оптимізувати оборонну логістику й ресурсного забезпечення завдяки впровадженню інтелектуальних систем обліку та розподілу майна, прогнозуванню потреб підрозділів у боєприпасах і матеріальних засобах, а також предиктивному обслуговуванню військової техніки на основі її фактичного зносу. Елементом цього етапу виступають технологічні платформи інтеграції Defense-tech, які виступають

державними цифровими майданчиками для прискореної апробації, тестування та впровадження готових AI-рішень приватного сектору (вітчизняних Military-tech стартапів) у наявні аналітичні та управлінські комплекси Збройних Сил України [21].

Одночасно на вертикальному рівні штучний інтелект забезпечує динамічне узгодження стратегічних директив РНБО із практичною діяльністю бойових підрозділів, створюючи алгоритмічний зворотний зв'язок.

Використання інтелектуальних систем ситуаційної обізнаності та автоматизованих систем управління дозволяє в режимі реального часу здійснювати синхронізацію дій різних видів і родів військ, спецслужб та правоохоронних органів при виконанні спільних завдань із протидії воєнним, кібернетичним та інформаційно-психологічним загрозам. Завдяки ШІ-системам SPECTR військові зможуть швидше взаємодіяти з інформацією з поля бою, при цьому дані залишатимуться у захищеному периметрі [52; 122].

Важливе значення, на переконання О. Вольської, тут має розвиток публічно-приватного партнерства, яке дає змогу залучати експертизу, технології та інвестиції приватних IT-компаній і вітчизняних AI-розробників до виконання державних завдань у сфері оборони та кіберзахисту [21]. На цьому ж етапі здійснюється пряме державне грантове фінансування (зокрема через оборонний кластер BRAVE1), цільове оборонне замовлення, запровадження спеціальних податкових режимів для Military-tech розробників, а також адаптацію процедур державних закупівель до специфіки високотехнологічних і ризикових AI-проєктів [21].

Інтеграція технологій ШІ в системи управління (такі як Delta чи Кропива) перетворює координацію на автоматизований процес ситуаційної обізнаності, де всі підрозділи й суб'єкти управління бачать єдину, актуалізовану в режимі реального часу картину оперативної обстановки. Фактично йдеться про створення єдиної цифрової екосистеми управління ресурсами – від стратегічного рівня Міністерства оборони до окремих військових частин. Система дозволяє автоматизувати ключові процеси, зменшити вплив людського фактору,

скоротити бюрократію та забезпечити прозорість управління ресурсами в режимі реального часу [146].

Завершальним елементом управлінського циклу є етап контролю, де технології штучного інтелекту забезпечують перехід від формального паперового аудиту до безперервного, автоматизованого та дата-центричного моніторингу результативності публічного управління. За допомогою аналізу великих масивів даних (Big Data) ШІ-системи здійснюють моніторинг у режимі реального часу стану виконання державних оборонних програм, ефективності використання бюджетних коштів та матеріально-технічних ресурсів, а також дотримання графіків постачання озброєння та військової техніки. Завдяки алгоритмам предиктивної аналітики система здатна виявляти відхилення від запланованих індикаторів ефективності та ризики корупційних чи логістичних збоїв ще на ранніх стадіях їх виникнення. Крім того, ШІ забезпечує об'єктивний аналіз бойового застосування імплементованих технологій (оцінку ефективності алгоритмів розвідки, систем підтримки прийняття рішень та автономних комплексів безпосередньо в умовах воєнних дій), створюючи емпіричну базу для подальшого коригування етапів прогнозування та планування для нового публічно-управлінського циклу.

На підставі проведеного аналізу можна зробити висновок, що імплементація технологій штучного інтелекту в систему публічного управління обороноздатністю України зумовлює якісну трансформацію всього управлінського циклу – від прогнозування та планування до безперервного контролю [123]. Застосування сучасних ШІ-інструментів, зокрема систем підтримки прийняття рішень, алгоритмів семіотичного аналізу та обробки мультидоменних розвідувальних даних у режимі реального часу, дозволяє подолати інертність традиційних бюрократичних структур і забезпечити перехід від реактивного управління до випереджального (предиктивного), адаптивного та дата-центричного. Це гарантує оперативне реагування на воєнно-технологічні виклики, оптимізацію ресурсного забезпечення через програмне моделювання, дотримання етичних і правових норм ведення оборони та суттєве підвищення

загальної інституційної спроможності сектору безпеки і оборони України. У контексті забезпечення обороноздатності України ефективність вимірюється швидкістю управлінського циклу: чим менше часу витрачається на міжвідомче регулювання й координацію, тим вищою є адаптивність і стійкість всієї держави перед обличчям агресора.

Циклічність етапів публічного управління може стати підставою для побудови схеми інтеграції інструментів штучного інтелекту (ШІ) в систему публічного управління оборонним сектором України (рис. 2.7). Вона наочно відображає структурно-функціональний зв'язок між зовнішніми викликами, внутрішніми етапами управлінського циклу та підсумковими стратегічними результатами.

Рис. 2.7. Інтеграція інструментів штучного інтелекту (ШІ) в систему публічного управління оборонним сектором України

Джерело: створено автором на основі проведеного аналізу

На схемі чітко видно, що публічне управління у сфері обороноздатності детермінується зовнішнім середовищем з його екзистенційними загрозами та цивілізаційними цінностями. Це стає базовим імпульсом та цільовою установкою для всієї системи управління та визначає, що використанні ШІ в системі публічного управління не є самоціллю. Застосування новітніх технологій

для забезпечення обороноздатності держави, її підсилення є необхідною відповіддю на виклики зовнішнього середовища задля збереження фундаментальних цивілізаційних засад держави.

Центральна частина схеми відображає циклічний процес публічного управління та відображає його основні стадії: прогнозування та планування, програмування, організація та регулювання, координація та контроль.

Наступний блок (AI-посилення) відображає основні напрями втілення ШІ у публічне управління: аналітика даних та їх аналіз у режимі реального часу; автоматизація, тобто прискорення рутинних бюрократичних процедур та операційних процесів; оптимізація, яка зумовлює покращення розподілу ресурсів і підтримку прийняття рішень.

Блок «Трансформація парадигми управління» демонструє еволюційну траєкторію публічного управління від традиційної моделі до ШІ-інтегрованої моделі забезпечення обороноздатності, високоефективної, адаптивної та дата-центричної. Інтеграція інструментів штучного інтелекту на кожній із семи стадій управлінського циклу (прогнозування, планування, програмування, організація, регулювання, координація, контроль) дозволяє досягти синергетичного ефекту, забезпечуючи високу інституційну стійкість держави, безпеку та захист суверенітету при безумовному дотриманні принципів демократичного цивільного контролю.

І можна погодитись з позицією В. Василенка, який зазначає, що за таких умов перед системою публічного адміністрування постає необхідність досягнення оптимального балансу між стимулюванням технологічних інновацій та забезпеченням національної безпеки. Це передбачає встановлення дієвого контролю за функціонуванням алгоритмічних систем, гарантування високого рівня кіберзахисту й персональних даних, а також мінімізацію техніко-технологічних і управлінських похибок, здатних спричинити системні деструктивні наслідки. Впровадження інструментів штучного інтелекту в публічну сферу вимагає цілісного теоретико-методологічного осмислення – починаючи від етичних та правових засад до оцінювання ризиків і формування

механізмів гарантування безпеки. Відтак, наукова концептуалізація процесів інтеграції ШІ-технологій у публічне управління виступає критично важливим завданням для сучасної науки та практики, спрямованим на формування стійкої, надійної та високотехнологічної моделі цифрової держави [16].

Висновки до розділу 2.

У розділі 2 дисертаційного дослідження розглянуто чинну нормативно-правову базу використання ШІ для посилення обороноздатності України, виявлено існуючі прогалині і недоліки у регулюванні використання ШІ в оборонній та безпековій сферах.

Аналіз чинної нормативно-правової бази засвідчив, що існуючі стратегічні й програмні документи створюють загальну політичну основу для розвитку технологій штучного інтелекту та визначають його одним із пріоритетних напрямів. Водночас вони мають переважно декларативний характер і не встановлюють юридично обов'язкових вимог до розроблення та застосування оборонних ШІ-систем. Відсутність спеціалізованого закону або галузевої стратегії застосування штучного інтелекту в оборонній сфері свідчить про наявність системної прогалини в законодавстві. Зокрема, поняття «автономні системи озброєння», рівні людського контролю та «критичні функції» зброї залишаються законодавчо не врегульованими, що ускладнює формування технічних вимог, укладення договорів і встановлення правомірності їх використання. У цьому контексті стратегічне значення має розробка Проєкту Закону України «Про правове регулювання штучного інтелекту», а також гармонізація вітчизняного законодавства з міжнародними стандартами та Регламентом ЄС про штучний інтелект із дотриманням принципів конституційності та верховенства права.

З'ясовано, що цілісна інституційна архітектура регулювання та забезпечення штучного інтелекту в сфері обороноздатності України формується за участю Кабінету Міністрів України як стратегічного координатора, Міністерства цифрової трансформації України як головного органу у сфері

цифрової політики, спеціального цифрового регулятора, органів ринкового нагляду, CERT-UA та Міністерства оборони України. Для підвищення ефективності публічного управління запропоновано розглядати інституційну архітектуру управління обороноздатністю країни крізь призму п'яти взаємопов'язаних функціональних блоків: політико-законодавчого, виконавчо-координаційного, безпеково-інфраструктурного, оперативно-застосовного та інноваційно-технологічного з обов'язковим включенням освітньо-наукового компонента. Для подолання розпорошеності повноважень обґрунтовано доцільність створення міжвідомчого координаційного центру за участю Міністерства оборони, Генерального штабу ЗСУ, Мінцифри та інших уповноважених суб'єктів для формування узгодженої політики та посилення міжнародного співробітництва.

Зазначається, що суб'єкти публічного управління у сфері забезпечення обороноздатності взаємодіють між собою по вертикалі та по горизонталі, у відповідності до статусу у суспільстві, міри підпорядкування, функціональних обов'язків та повноважень, які вони виконують. При цьому вертикальні зв'язки відображають відносини підпорядкованості, нормотворення та стратегічного контролю, а горизонтальні – оперативну координацію, обмін даними, спільну R&D-діяльність та міжвідомчу синергію.

Доведено, що імплементація технологій штучного інтелекту зумовлює якісну трансформацію цілісного управлінського циклу: від прогнозування та планування до координації та безперервного контролю. Застосування інструментів штучного інтелекту, зокрема систем підтримки прийняття рішень, алгоритмів аналізу та обробки мультидоменних розвідувальних даних у режимі реального часу, дозволяє подолати інертність традиційних бюрократичних структур і забезпечити перехід від реактивного управління до випереджального (предиктивного), адаптивного та дата-центричного. В умовах воєнного стану ефективність публічного управління вимірюється швидкістю управлінського циклу: скорочення часу на міжвідомче регулювання й координацію безпосередньо підвищує адаптивність та стійкість всієї системи національної

безпеки.

Визначено першочергові заходи для вдосконалення інституційно-правових засад впровадження штучного інтелекту в секторі безпеки і оборони України. До них належать: систематизація понятійно-категоріального апарату в законодавстві; розробка й затвердження галузевої концепції застосування ШІ в обороні відповідно до світових стандартів; запровадження механізму правової оцінки засобів ведення війни на основі ШІ; встановлення уніфікованих стандартів тестування, сертифікації, аудиту та спеціальних вимог кібербезпеки (зокрема захисту від отруєння даних і змагальних атак у системах на кшталт «SPECTR» та БПЛА); нормативне врегулювання порядку використання військових масивів даних; а також унормування типових договірних умов оборонних закупівель щодо прав на моделі ШІ та інтелектуальну власність. Обов'язковими заходами для покращення та вдосконалення інституційних засад впровадження штучного інтелекту в секторі безпеки і оборони України повинні стати заходи з забезпечення належного рівня підготовки персоналу: організація навчання для командирів, операторів і юристів, уповноважених здійснювати правовий огляд та оцінювати використання ШІ, підвищення кваліфікації представників публічного управління. Комплексна реалізація цих заходів підсилить інституційну спроможність держави та забезпечить надійне функціонування оборонного сектору України.

Встановлено, що інтеграцію ШІ-рішень задля підвищення обороноздатності України доцільно аналізувати крізь призму цілісного управлінського циклу: прогнозування, планування, програмування, організації, регулювання, координації та контролю. Послідовне залучення штучного інтелекту на всіх етапах публічного управління виступає об'єктивно зумовленим кроком. По-друге, зазначені етапи формують єдину циклічну систему, де кожен елемент взаємопов'язаний із наступним та реагує на виклики зовнішнього середовища. В екстремальних умовах воєнного стану чіткі межі між цими стадіями трансформуються, гарантуючи управлінському процесу адаптивність, високу

Отже, аналіз наукової літератури та сучасних реалій дозволив зробити висновок про те, що в умовах воєнного стану публічне управління модернізується, трансформується, стає більш адаптивним та гнучким, обираючи нетрадиційні методи та способи. Висока внутрішня мотивація до публічної служби сприяє підвищенню обороноздатності держави.

На підставі проведеного аналізу можна зробити висновок, що імплементація технологій штучного інтелекту в систему публічного управління обороноздатністю України зумовлює якісну трансформацію всього управлінського циклу – від прогнозування та планування до безперервного контролю. Застосування сучасних ШІ-інструментів, зокрема систем підтримки прийняття рішень, алгоритмів семіотичного аналізу та обробки мультидоменних розвідувальних даних у режимі реального часу, дозволяє подолати інертність традиційних бюрократичних структур і забезпечити перехід від реактивного управління до випереджального (предиктивного), адаптивного та дата-центричного. Це гарантує оперативне реагування на воєнно-технологічні виклики, оптимізацію ресурсного забезпечення через програмне моделювання, дотримання етичних і правових норм ведення оборони та суттєве підвищення загальної інституційної спроможності сектору безпеки і оборони України. У контексті забезпечення обороноздатності України ефективність вимірюється швидкістю управлінського циклу: чим менше часу витрачається на міжвідомче регулювання й координацію, тим вищою є адаптивність і стійкість всієї держави перед обличчям агресора.

Циклічність етапів публічного управління може стати підставою для побудови схеми інтеграції інструментів штучного інтелекту (ШІ) в систему публічного управління оборонним сектором України (рис. 2.7). Вона наочно відображає структурно-функціональний зв’язок між зовнішніми викликами, внутрішніми етапами управлінського циклу та підсумковими стратегічними результатами.

РОЗДІЛ ІІІ
НАПРЯМИ ВДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

3.1. Зарубіжний досвід публічного управління використання штучного інтелекту для підвищення обороноздатності держави

У сучасних умовах штучний інтелект перетворюється на важливий інструмент зміцнення обороноздатності держави, значення якого виходить за межі суто технологічного забезпечення діяльності сектору безпеки і оборони. Його впровадження відкриває нові можливості для підвищення ефективності стратегічного планування, інформаційно-аналітичного забезпечення, прогнозування безпекових загроз, оперативності ухвалення управлінських рішень та координації діяльності суб'єктів сектору безпеки і оборони. Водночас результативність використання таких технологій залежить не лише від рівня їх розвитку, а й від спроможності держави сформувати належні організаційні, нормативно-правові та інституційні умови для їх інтеграції в систему оборонного управління [124].

У цьому контексті міжнародний досвід засвідчує поступовий перехід від сприйняття штучного інтелекту як окремого технологічного рішення до його розгляду як складової системної трансформації оборонного управління. Показовим є підхід НАТО, відповідно до якого штучний інтелект розглядається як технологія, здатна впливати на різні напрями діяльності Альянсу, зокрема колективну оборону та реагування на кризи. В оновленій Стратегії штучного інтелекту НАТО 2024 р. наголошено на необхідності прискорення впровадження ШІ, забезпечення сумісності відповідних систем держав-членів, інтеграції з іншими передовими технологіями та поглиблення співпраці з промисловістю й академічною спільнотою [202]. Актуалізуються питання узгодженості стратегічних пріоритетів, міжінституційної взаємодії та формування дієвих

механізмів державного управління впровадженням штучного інтелекту у сфері оборони.

Специфіка зарубіжного досвіду полягає в тому, що держави обирають різні підходи до інтеграції штучного інтелекту в оборонну сферу з огляду на масштаби економіки, організацію збройних сил, рівень технологічного розвитку, демографічні особливості, характер безпекових викликів і стан національної оборонної промисловості. Одні країни зосереджуються на формуванні власної технологічної та науково-дослідної основи, інші на співпраці з приватним бізнесом і міжнародними партнерами, а треті на розвитку автономних платформ, розвідувальних рішень або цифровізації системи командування. Водночас для всіх спільним є прагнення перейти від поодиноких експериментів зі ШІ до його комплексного застосування у військовому управлінні. Отже, міжнародна практика засвідчує, що результативність використання штучного інтелекту для зміцнення обороноздатності визначається не лише досконалістю алгоритмів, а й спроможністю держави забезпечити належну інфраструктуру даних, цифрові комунікаційні мережі, кваліфікований персонал, дієві управлінські механізми, промисловий потенціал і процедури контролю.

Дослідження зарубіжного досвіду використання штучного інтелекту для підвищення обороноздатності держави потребує врахування не лише технологічних напрямів його застосування, а й особливостей організації публічного управління відповідними процесами. У цьому контексті важливого значення набуває визначення управлінських підходів, інституційних механізмів, форм міжвідомчої взаємодії, способів ресурсного забезпечення та інструментів державної підтримки впровадження інтелектуальних технологій у секторі безпеки і оборони. У ході дисертаційної роботи ми будемо розглядати зарубіжний досвід з позицій його потенційної придатності для вдосконалення системи публічного управління забезпеченням обороноздатності України.

Для проведення порівняльного аналізу обрано досвід п’яти країн Австралії, Великої Британії, Франції, Японії та Ізраїлю. Вибір зазначених держав зумовлений різноманітністю організаційних і управлінських підходів до

розвитку оборонного штучного інтелекту, особливостями їхнього безпекового середовища, рівнем залучення державних інституцій, оборонної промисловості, наукових установ і приватного сектору до впровадження інтелектуальних технологій. Аналіз досвіду цих країн дозволяє виявити як спільні закономірності розвитку публічного управління використання ШІ, так і специфічні управлінські рішення, сформовані відповідно до національних оборонних потреб та інституційних можливостей.

Порівняльний аналіз зарубіжного досвіду доцільно здійснювати за такими критеріями: стратегічне забезпечення розвитку та використання штучного інтелекту в оборонній сфері; інституційна організація та розподіл управлінських повноважень; організаційні механізми впровадження інтелектуальних технологій; ресурсне, кадрове та технологічне забезпечення; управління ризиками й забезпечення відповідального застосування ШІ; можливості адаптації відповідних управлінських практик до національних умов України. Застосування зазначених критеріїв дозволяє забезпечити системність порівняння та визначити не лише особливості зарубіжних моделей, а й їхні управлінські елементи, що можуть становити практичний інтерес для підвищення обороноздатності України.

Показовим у контексті дослідження зарубіжного досвіду публічного управління використання штучного інтелекту для підвищення обороноздатності держави є досвід Австралії, особливістю якого виступає поєднання стратегічного державного планування, міжнародного технологічного партнерства та практичного впровадження інновацій у діяльність оборонного сектору. Стратегічні засади відповідних процесів визначаються Національною оборонною стратегією Австралії 2024 року (2024 National Defence Strategy), у якій розвиток сучасних технологій розглядається в контексті модернізації оборонної системи та формування інтегрованих оборонних спроможностей [164]. Важливого значення набуває узгодження стратегічних пріоритетів, технологічних можливостей та ресурсного забезпечення відповідно до потреб національної оборони.

Важливу роль у науково-технологічному забезпеченні оборонної діяльності відіграє Defence Science and Technology Group (DSTG), яка сприяє проведенню досліджень, випробуванню перспективних технологій та взаємодії між державними структурами, науковим середовищем і міжнародними партнерами. Зокрема, у 2024 році в межах «The Technical Cooperation Program AI Strategic Challenge» було організовано випробування технологій штучного інтелекту за участю фахівців п'яти держав [161]. Такі заходи демонструють вагоме значення організаційних механізмів апробації технологій, спільного оцінювання їхніх можливостей та формування підстав для прийняття рішень щодо подальшого впровадження інновацій в оборонній сфері.

Характерною особливістю австралійського підходу є використання міжнародного технологічного співробітництва, насамперед у межах партнерства AUKUS між Австралією, Великою Британією та США. Другий напрям цього партнерства (AUKUS Pillar II) охоплює розвиток передових оборонних технологій, зокрема штучного інтелекту й автономних систем [163]. Практичним прикладом відповідної співпраці є випробування технологій машинного навчання для аналізу інформації про підводну обстановку, що надходить від гідроакустичних буїв, зокрема з використанням патрульних літаків P-8A Poseidon. Зазначена практика свідчить про можливості міжнародного партнерства як інструменту об'єднання технологічних і ресурсних спроможностей, організації спільних випробувань та інтеграції інновацій у наявні оборонні системи.

Водночас австралійський підхід передбачає поєднання технологічного розвитку з формуванням засад відповідального використання штучного інтелекту. У документі Міністерства оборони Австралії «Policy Settings for Responsible Use of Artificial Intelligence in Defence» визначено підходи до управління ризиками, забезпечення надійності та безпеки інтелектуальних систем, дотримання правових вимог і збереження відповідальності людини за прийняття рішень [164]. Виникає необхідність інтеграції процедур контролю й

оцінювання ризиків у процеси розроблення, випробування та практичного застосування оборонних технологій.

Подальший розвиток зазначених підходів відображено в Defence Digital Strategy and Roadmap 2025, у межах якої цифрова трансформація оборонної сфери пов'язується з розвитком захищеної цифрової інфраструктури, використанням даних та вдосконаленням технологічних спроможностей [162]. Отже, досвід Австралії характеризується стратегічно-координаційним підходом до публічного управління використання штучного інтелекту, що передбачає узгодження оборонних пріоритетів із технологічним розвитком, науково-технологічне забезпечення інновацій, міжнародне партнерство та впровадження процедур відповідального застосування ШІ.

Важливе місце в дослідженні зарубіжного досвіду публічного управління використання штучного інтелекту для підвищення обороноздатності держави посідає Велика Британія, підхід якої характеризується орієнтацією на формування інституційної готовності оборонного сектору до системного впровадження інтелектуальних технологій. Стратегічні засади відповідних процесів визначено у Стратегії штучного інтелекту у сфері оборони (Defence Artificial Intelligence Strategy), ухваленій Міністерством оборони Великої Британії у 2022 році. Документ передбачає чотири взаємопов'язані напрями: формування організаційної готовності оборонного сектору до використання ШІ (AI ready), прискорення та масштабування його впровадження, розвиток оборонної екосистеми штучного інтелекту та участь у формуванні міжнародних підходів до відповідального застосування інтелектуальних технологій [221]. Зазначені напрями відображають комплексний підхід до узгодження стратегічного планування, організаційного розвитку та технологічної модернізації оборонного сектору.

Визначальною особливістю британської практики є пріоритетність формування організаційної готовності до використання штучного інтелекту, що передбачає вдосконалення управлінських процесів, розвиток цифрової інфраструктури, належну організацію роботи з даними та підвищення

професійних компетентностей персоналу. Особливого значення набуває кадрове забезпечення, зокрема підготовка фахівців, здатних розробляти, впроваджувати й оцінювати інтелектуальні технології, а також розвиток відповідних навичок серед керівного складу оборонних структур [221]. Отже, чітко простежується, що результативність використання ШІ залежить не лише від наявності технологічних рішень, а й від спроможності державних інституцій інтегрувати їх у процеси виконання управлінських функцій.

Важливою складовою британського підходу є формування оборонно-технологічної екосистеми шляхом розвитку взаємодії між державними органами, оборонною промисловістю, приватними технологічними компаніями та науково-дослідними установами. Залучення недержавних суб'єктів до розроблення інтелектуальних технологій сприяє розширенню інноваційних можливостей оборонного сектору та створює передумови для прискорення переходу від експериментальних розробок до практичного застосування, що вказує на вагоме значення партнерських механізмів, у межах яких держава визначає пріоритетні оборонні потреби, забезпечує організаційні умови співпраці та координує впровадження технологічних рішень відповідно до завдань оборонної політики.

Окремого значення набуває забезпечення відповідального використання штучного інтелекту, що передбачає врахування правових та етичних вимог, управління ризиками, забезпечення належного людського контролю й визначення відповідальності за результати застосування інтелектуальних систем. У британській стратегії відповідальне використання ШІ розглядається як необхідна складова його впровадження в оборонній сфері [222]. Водночас розвиток британської оборонної політики характеризується посиленням уваги до прискорення технологічних інновацій та адаптації управлінських процедур до змін сучасного безпекового середовища актуалізує необхідність узгодження темпів упровадження технологій із вимогами їхньої надійності, безпеки та підконтрольності.

Отже, британський досвід характеризується інституційно-організаційним підходом до публічного управління використання штучного інтелекту в

оборонній сфері, визначальними рисами якого є формування організаційної готовності оборонних інституцій, розвиток кадрового потенціалу, розбудова оборонно-технологічної екосистеми та створення умов для масштабування інновацій. Зазначений підхід демонструє значення поєднання технологічної модернізації з удосконаленням управлінських процесів, розвитком професійних компетентностей і забезпеченням відповідального застосування ШІ для підвищення обороноздатності держави.

Важливе значення для дослідження зарубіжного досвіду публічного управління використання штучного інтелекту для підвищення обороноздатності держави має практика Франції, характерною особливістю якої є поєднання централізованої державної координації розвитку інтелектуальних технологій із забезпеченням технологічного суверенітету та формуванням власних оборонних спроможностей. Стратегічні засади відповідних процесів визначено в міністерській стратегії розвитку штучного інтелекту в оборонній сфері, представленій Міністерством збройних сил Франції у березні 2024 року. Її основним спрямуванням є розширення використання інтелектуальних технологій у діяльності збройних сил, розвиток національного науково-технологічного потенціалу та створення організаційних умов для практичного впровадження інновацій [198]. Вищевказане відображає прагнення держави забезпечити узгодженість стратегічного планування, інституційного забезпечення та технологічної модернізації оборонного сектору.

Однією з визначальних особливостей французької моделі є орієнтація на технологічний суверенітет, що передбачає розвиток власних алгоритмічних рішень, обчислювальної інфраструктури, систем управління даними та кадрового потенціалу [196]. Устаткована орієнтація вказує на зменшення критичної залежності від зовнішніх технологічних постачальників і забезпечення спроможності держави самостійно визначати пріоритети використання інтелектуальних технологій відповідно до потреб національної оборони. Технологічний суверенітет виступає важливим орієнтиром державної оборонної політики, який потребує узгодження інвестиційної діяльності,

розвитку наукових досліджень та забезпечення захищеності інформаційних ресурсів оборонного призначення.

Важливим інституційним рішенням стало створення у травні 2024 року Агентства Міністерства збройних сил Франції з питань штучного інтелекту в оборонній сфері (Agence ministérielle pour l'intelligence artificielle de défense, AMIAD), призначеного для координації розвитку та впровадження інтелектуальних технологій відповідно до потреб збройних сил [195]. Діяльність агентства спрямована на поєднання наукових досліджень, технологічних розробок і практичних потреб оборонного сектору. Подальшим кроком стало відкриття у березні 2025 року дослідницького центру AMIAD на кампусі «École polytechnique», що сприяє розвитку науково-технологічного потенціалу та взаємодії державних інституцій, дослідницьких установ і технологічних компаній, де показано важливе значення спеціалізованого організаційного механізму, здатного забезпечувати координацію оборонних інновацій, концентрацію ресурсів та послідовність переходу від наукових розробок до практичного використання [197].

Французький підхід передбачає комплексне використання штучного інтелекту у військових операціях, бортових та інших вбудованих системах, а також у внутрішніх організаційних процесах оборонного відомства [196]. Особливого значення набуває останній напрям, оскільки він створює можливості для вдосконалення інформаційно-аналітичного забезпечення, оптимізації управлінських процедур, планування ресурсів і підтримки прийняття рішень. Водночас результативність застосування ШІ залежить від належної організації роботи з даними, розвитку цифрової інфраструктури, підготовки персоналу та узгодження технологічних рішень із функціональними потребами оборонного сектору.

Отже, досвід Франції характеризується централізовано-інституційним підходом до публічного управління використання штучного інтелекту в оборонній сфері, визначальними рисами якого є посилена роль держави у формуванні стратегічних пріоритетів, функціонування спеціалізованої

структури координації, розвиток національного технологічного потенціалу та забезпечення взаємозв'язку між науковими дослідженнями, оборонною промисловістю і практичними потребами збройних сил.

Особливе місце серед зарубіжних практик публічного управління використання штучного інтелекту для підвищення обороноздатності держави посідає досвід Японії, характерною рисою якого є поєднання технологічної модернізації оборонного сектору з необхідністю подолання демографічних обмежень та підвищення ефективності використання людських ресурсів. Стратегічні засади відповідних процесів визначено в Основній політиці щодо сприяння використанню штучного інтелекту (Basic Policy on Promoting AI Utilization), оприлюдненій Міністерством оборони Японії в липні 2024 року. Документ визначає пріоритетні напрями застосування інтелектуальних технологій у діяльності оборонного відомства та Сил самооборони Японії, зокрема для вдосконалення інформаційно-аналітичного забезпечення, підвищення ефективності виконання завдань та розвитку оборонних спроможностей [189], а також прагнення держави узгодити технологічний розвиток із функціональними потребами оборонного сектору та наявними ресурсними можливостями.

Одним із визначальних чинників розвитку оборонного штучного інтелекту в Японії виступають демографічні зміни, зокрема старіння населення та скорочення чисельності працездатних осіб, що створюють довгострокові обмеження для кадрового забезпечення Сил самооборони. Через те використання ШІ спрямовується на автоматизацію повторюваних операцій, зменшення навантаження на персонал, прискорення оброблення інформації та підвищення продуктивності діяльності військових структур [189]. Простежуються можливості застосування інтелектуальних технологій як інструменту адаптації оборонного управління до кадрових і ресурсних обмежень без необхідності пропорційного збільшення чисельності персоналу.

Важливою складовою японського підходу є використання штучного інтелекту для вдосконалення інформаційно-аналітичних, організаційних і

ресурсних процесів. Застосування відповідних технологій створює можливості для автоматизованого аналізу значних обсягів інформації, підтримки прийняття управлінських рішень, оптимізації логістичного забезпечення та виконання окремих адміністративних функцій. Особливого значення набуває підвищення результативності використання наявних ресурсів, скорочення часу виконання повторюваних операцій та забезпечення своєчасності управлінських рішень. Водночас результативність таких процесів залежить від розвитку цифрової інфраструктури, належної організації роботи з даними та професійної підготовки персоналу.

Окремого значення в японській практиці набуває забезпечення відповідального використання штучного інтелекту. У червні 2025 року Міністерство оборони Японії оприлюднило Guidelines on Responsible Application of AI in Research and Development of Defense Equipment, спрямовані на врахування правових, етичних і безпекових вимог під час дослідження та розроблення оборонних технологій [188]. Вищезазначене демонструє важливість інтеграції процедур оцінювання ризиків, забезпечення надійності інтелектуальних систем і належного людського контролю на ранніх етапах їх створення. Тут ми розглядаємо відповідальне використання ШІ як складову управлінського процесу, а не лише як завершальний етап перевірки технологічних рішень.

Досвід Японії характеризується ресурсно-адаптивним підходом із ризик-орієнтованим компонентом до публічного управління використання штучного інтелекту в оборонній сфері, визначальними рисами якого є орієнтація на подолання кадрових і ресурсних обмежень, підвищення продуктивності діяльності оборонних структур, удосконалення інформаційно-аналітичного забезпечення та формування процедур відповідального застосування інтелектуальних технологій. Відбувається процес узгодження технологічної модернізації з довгостроковими потребами оборонного планування, ефективним використанням ресурсів і забезпеченням надійності управлінських рішень.

Досвід Ізраїлю становить особливий інтерес у контексті дослідження публічного управління використання штучного інтелекту для підвищення обороноздатності держави, оскільки характеризується поєднанням розвитку оборонних інновацій, тісної взаємодії державних структур із технологічним сектором та орієнтації на оперативне впровадження новітніх розробок відповідно до потреб національної безпеки. В умовах тривалих безпекових загроз штучний інтелект розглядається як інструмент удосконалення інформаційно-аналітичного забезпечення, розвитку оборонних спроможностей та підвищення результативності використання наявних ресурсів. З позицій публічного управління характерною особливістю ізраїльського підходу є формування організаційних механізмів, спрямованих на забезпечення взаємозв'язку між державним оборонним плануванням, науково-технологічними дослідженнями та практичними потребами збройних сил.

Важливим інституційним рішенням стало створення наприкінці 2024 року спеціалізованого Управління штучного інтелекту та автономних систем (AI and Autonomy Administration), про початок діяльності якого Міністерство оборони Ізраїлю офіційно повідомило 1 січня 2025 року. Зазначена структура функціонує в межах Управління оборонних досліджень і розробок (Directorate of Defense Research and Development, DDR&D) та покликана забезпечувати координацію досліджень, розроблення й розвитку спроможностей у сфері штучного інтелекту та автономних систем для різних видів збройних сил [186]. Її діяльність передбачає залучення фахівців військових технологічних підрозділів, наукових установ, оборонної промисловості та інноваційних компаній, створення спеціалізованої структури демонструє значення інституційної координації та концентрації науково-технологічних ресурсів для прискорення розвитку оборонних інновацій [178].

Визначальною особливістю ізраїльської практики є розвиток оборонно-інноваційної екосистеми, у межах якої взаємодіють Міністерство оборони, збройні сили, науково-дослідні установи, великі технологічні компанії та стартапи. Так, створюються передумови для залучення результатів цивільних

технологічних розробок до виконання оборонних завдань, оперативного визначення перспективних рішень та організації їх випробування. З позицій публічного управління особливого значення набувають механізми узгодження потреб військових структур із можливостями розробників, координація інноваційних проєктів і забезпечення переходу від дослідницьких результатів до практичного застосування. Відповідна організація взаємодії сприяє підвищенню адаптивності оборонного сектору до змін безпекового середовища [187].

Водночас інтенсивне впровадження штучного інтелекту в оборонній сфері супроводжується ризиками, пов'язаними з достовірністю алгоритмічних результатів, прозорістю процесів прийняття рішень, визначенням відповідальності та забезпеченням належного людського контролю. Особливого значення визначені питання набувають під час використання інтелектуальних систем для оброблення розвідувальної інформації та підтримки рішень, здатних мати істотні наслідки для життя і безпеки людей. Виникає необхідність поєднання прискореного впровадження оборонних інновацій із процедурами перевірки надійності технологій, оцінювання ризиків, дотримання вимог міжнародного гуманітарного права та забезпечення відповідальності уповноважених суб'єктів за прийняті рішення [187].

Отже, досвід Ізраїлю характеризується партнерсько-інноваційним підходом до публічного управління використання штучного інтелекту в оборонній сфері, визначальними рисами якого є тісна взаємодія державних і недержавних суб'єктів, інституційна координація оборонних досліджень, орієнтація на оперативне впровадження технологічних розробок та адаптація інноваційних процесів до актуальних безпекових потреб. Водночас зазначений досвід демонструє необхідність забезпечення належного управлінського контролю за використанням інтелектуальних систем, особливо в умовах їх застосування для підтримки критично важливих оборонних рішень.

Порівняння досвіду аналізованих держав свідчить, що використання штучного інтелекту для підвищення обороноздатності характеризується різноманітністю підходів до організації публічного управління відповідними

процесами. Попри відмінності у стратегічних пріоритетах, інституційній організації та ресурсних можливостях, спільною рисою зазначених підходів є прагнення забезпечити узгодженість технологічного розвитку з потребами оборонного сектору, підвищити результативність управлінських рішень та створити організаційні передумови для практичного впровадження інновацій.

З метою систематизації зарубіжного досвіду та визначення особливостей публічного управління використання штучного інтелекту в оборонній сфері здійснено порівняльний аналіз за критеріями стратегічного забезпечення, інституційної організації, механізмів упровадження, ресурсного забезпечення та управління ризиками. Результати проведеного аналізу узагальнено в табл. 3.1.

Таблиця 3.1

Порівняльна характеристика підходів до публічного управління використання штучного інтелекту в оборонній сфері зарубіжних держав

Держава	Характерні особливості публічного управління	Основні механізми реалізації	Управлінський пріоритет
Австралія	Узгодження оборонного планування з технологічним розвитком і міжнародним співробітництвом	Стратегічне планування, DSTG, партнерство AUKUS, спільні випробування	Координація технологічних інновацій
Велика Британія	Формування організаційної готовності оборонного сектору до системного використання ШІ	Defence AI Strategy, розвиток компетентностей, державно-приватне партнерство	Інституційна спроможність і масштабування інновацій
Франція	Централізована координація розвитку оборонного ШІ та забезпечення технологічного суверенітету	AMIAD, державна підтримка досліджень, розвиток власної технологічної інфраструктури	Концентрація управлінських і технологічних ресурсів
Японія	Адаптація оборонного управління до кадрових обмежень і вимог відповідального використання ШІ	Державна політика використання ШІ, автоматизація процесів, настанови щодо управління ризиками	Оптимізація ресурсів і надійність технологій
Ізраїль	Інтеграція державного оборонного управління з інноваційною екосистемою	AI and Autonomy Administration, взаємодія з оборонною промисловістю та технологічними компаніями	Прискорення розроблення та впровадження інновацій

Джерело: сформовано автором на основі власних досліджень

Узагальнення результатів порівняльного аналізу, представлених у табл. 3.1, дозволяє встановити, що відмінності зарубіжних практик використання штучного інтелекту в оборонній сфері визначаються не лише рівнем технологічного розвитку держав, а й особливостями організації публічного управління відповідними процесами. Зокрема, австралійський досвід характеризується пріоритетністю стратегічної координації та міжнародного технологічного партнерства, британський – формуванням інституційної готовності до впровадження інтелектуальних технологій, французький – централізацією організаційного забезпечення та орієнтацією на технологічний суверенітет, японський – адаптацією управлінських процесів до ресурсних обмежень, а ізраїльський – розвитком партнерських механізмів прискореного впровадження оборонних інновацій.

Виявлені особливості дають підстави виокремити п’ять домінантних управлінських підходів до використання штучного інтелекту для підвищення обороноздатності держави: стратегічно-координаційний, інституційно-організаційний, централізовано-інституційний, ресурсно-адаптивний та партнерсько-інноваційний. Зазначені підходи не є взаємовиключними, оскільки в практиці окремих держав можуть одночасно застосовуватися різні організаційні та управлінські механізми. Їх розмежування здійснено за критерієм переважного управлінського пріоритету, що дозволяє визначити специфіку організації державного впливу на процеси розвитку та впровадження оборонного штучного інтелекту.

Водночас порівняльний аналіз свідчить про наявність спільних складових публічного управління використання штучного інтелекту, до яких належать стратегічне визначення пріоритетів, організаційна координація, науково-технологічне та кадрове забезпечення, взаємодія державних і недержавних суб’єктів, а також оцінювання ризиків і результативності впровадження інтелектуальних технологій. Відмінності між проаналізованими державами полягають насамперед у способах організації зазначених складових,

співвідношенні централізованих і партнерських механізмів та визначенні пріоритетних напрямів використання наявних ресурсів.

Практичне значення отриманих результатів полягає у можливості використання окремих управлінських механізмів зарубіжних держав для вдосконалення публічного управління застосуванням штучного інтелекту в секторі безпеки і оборони України. Водночас їх адаптація потребує врахування національних оборонних пріоритетів, інституційних і ресурсних можливостей, особливостей міжвідомчої взаємодії та вимог відповідального використання інтелектуальних технологій в умовах воєнного стану.

Враховуючи результати систематизації зарубіжних управлінських підходів, доцільно визначити пріоритетні напрями адаптації відповідного досвіду до потреб України. При цьому виокремлені п’ять підходів характеризують особливості організації публічного управління в проаналізованих державах, тоді як напрями адаптації відображають конкретні можливості вдосконалення управлінських механізмів у вітчизняному секторі безпеки і оборони. На цій основі обґрунтовано шість взаємопов’язаних напрямів, реалізація яких може сприяти підвищенню результативності використання штучного інтелекту для забезпечення обороноздатності України.

Першим перспективним напрямом є вдосконалення організаційної координації розвитку та використання штучного інтелекту в оборонній сфері. Досвід Франції та Ізраїлю демонструє значення спеціалізованих організаційних механізмів, здатних забезпечувати узгодження оборонних потреб із науково-технологічними розробками, координувати інноваційні проєкти та сприяти їх практичному впровадженню. Для України доцільним є посилення координації між органами державного управління, військовими структурами, науково-дослідними установами та розробниками оборонних технологій. При цьому йдеться не обов’язково про створення нового державного органу, а насамперед про чітке визначення відповідальних суб’єктів, розмежування їхніх функцій, удосконалення процедур взаємодії та формування узгодженого порядку визначення пріоритетів розвитку оборонного ШІ.

Другим напрямом є розвиток організаційних механізмів апробації, оцінювання та впровадження інтелектуальних технологій. Австралійський досвід засвідчує значення спільних технологічних випробувань і міжнародного партнерства, тоді як ізраїльська практика демонструє важливість оперативного узгодження розробок із практичними потребами оборонного сектору. Для України перспективним є вдосконалення управлінського процесу, що охоплює визначення оборонної потреби, відбір перспективних технологічних рішень, організацію їх випробувань, оцінювання результативності, прийняття рішення щодо впровадження та подальший моніторинг використання. Важливою умовою реалізації такого підходу є забезпечення зворотного зв'язку між військовими користувачами, розробниками та суб'єктами, відповідальними за управлінські рішення, що дозволяє своєчасно коригувати вимоги до технологій відповідно до змін оперативного середовища.

Третім напрямом є розвиток кадрового та організаційного потенціалу використання штучного інтелекту в секторі безпеки і оборони. Досвід Великої Британії та Японії підтверджує важливість поєднання технологічної модернізації з підготовкою персоналу, розвитком цифрових компетентностей і підвищенням ефективності використання людських ресурсів. Для України актуальним є формування диференційованих підходів до підготовки фахівців залежно від характеру їхніх управлінських і професійних функцій. Зокрема, доцільним є розвиток компетентностей керівного складу щодо можливостей, обмежень і ризиків використання ШІ, підготовка технічних фахівців із розроблення та супроводження інтелектуальних систем, а також навчання безпосередніх користувачів відповідних технологій. Це створюватиме організаційні передумови для результативного застосування ШІ без надмірного збільшення кадрового навантаження.

Четвертим напрямом є вдосконалення взаємодії держави з науковим середовищем, оборонною промисловістю та приватним технологічним сектором. Практика Великої Британії, Австралії та Ізраїлю свідчить про значення партнерських механізмів у розвитку оборонних інновацій. Для України

особливого значення набуває формування організаційних умов, які забезпечуватимуть залучення технологічних компаній, науково-дослідних установ і розробників до виконання пріоритетних оборонних завдань. У цьому контексті перспективними є вдосконалення механізмів визначення технологічних потреб, організації спільних досліджень, випробування інноваційних рішень та забезпечення їх подальшого впровадження. Водночас відповідна взаємодія має здійснюватися з урахуванням вимог захисту інформації, збереження прав інтелектуальної власності та забезпечення прозорого розподілу функцій і відповідальності між учасниками.

П’ятим напрямом є формування узгоджених процедур управління ризиками використання штучного інтелекту в оборонній сфері. Досвід Японії, Великої Британії та Австралії демонструє значення врахування вимог надійності, безпеки та відповідального застосування інтелектуальних технологій на різних етапах їхнього життєвого циклу. Для України доцільним є розвиток ризик-орієнтованого підходу, який передбачатиме оцінювання можливих наслідків застосування ШІ, перевірку достовірності алгоритмічних результатів, визначення належного рівня людського контролю та встановлення відповідальності уповноважених суб’єктів за прийняття рішень. Особливого значення такі процедури набувають під час використання інтелектуальних систем у процесах, пов’язаних із безпекою людей, обробленням чутливої інформації та підтримкою критично важливих оборонних рішень.

Шостим напрямом є забезпечення технологічної стійкості та зменшення критичної залежності від зовнішніх постачальників інтелектуальних технологій. Французький досвід засвідчує значення розвитку власного науково-технологічного потенціалу, захищеної цифрової інфраструктури та спроможностей управління даними. Для України перспективним є поєднання міжнародного технологічного співробітництва з підтримкою національних розробників, розвитком власних компетентностей у сфері штучного інтелекту та забезпеченням сумісності технологічних рішень із наявними оборонними системами. При цьому технологічна стійкість має розглядатися не як повна

відмова від іноземних технологій, а як здатність держави забезпечувати безперервність функціонування критично важливих систем, контролювати використання інформаційних ресурсів і зменшувати ризики залежності від окремих постачальників.

З метою узагальнення визначених напрямів адаптації зарубіжного досвіду систематизовано відповідні управлінські механізми, приклади їх реалізації в проаналізованих державах та очікувані результати застосування в Україні. Запропонована систематизація дозволяє встановити взаємозв'язок між особливостями зарубіжних практик публічного управління, можливостями їх використання у вітчизняному секторі безпеки і оборони та пріоритетними результатами вдосконалення управлінських процесів (рис. 3.1).

Представлена на рис. 3.1 систематизація дозволяє співвіднести визначені напрями адаптації зарубіжного досвіду з відповідними управлінськими механізмами та очікуваними результатами їх застосування в Україні. Її особливістю є функціональна орієнтація на вдосконалення публічного управління використання штучного інтелекту без механічного відтворення іноземних організаційних моделей.

Водночас практична реалізація запропонованих напрямів потребує диференційованого підходу з урахуванням інституційних, ресурсних і безпекових умов України. Зокрема, розвиток кадрових компетентностей, удосконалення міжвідомчої взаємодії, процедур випробування технологій та оцінювання ризиків можуть здійснюватися в межах діяльності наявних суб'єктів сектору безпеки і оборони. Натомість створення нових спеціалізованих інституцій, розгортання масштабної обчислювальної інфраструктури та реалізація довгострокових технологічних програм потребують додаткового обґрунтування щодо функціональної доцільності, ресурсного забезпечення й узгодженості з чинною системою державного управління.

Рис. 3.1. Напрями адаптації зарубіжного досвіду публічного управління використання штучного інтелекту для підвищення обороноздатності України

Джерело: власна розробка автора

Окремого значення в контексті адаптації зарубіжного досвіду набуває міжнародне оборонно-технологічне співробітництво. Практика Австралії та Великої Британії демонструє можливості використання партнерських механізмів для об'єднання науково-технологічних ресурсів, проведення спільних досліджень і випробувань, забезпечення технологічної сумісності та обміну досвідом. Для України міжнародне співробітництво доцільно розглядати як інструмент розвитку власних інституційних і технологічних спроможностей, а не як альтернативу формуванню національного оборонно-інноваційного потенціалу.

Важливою умовою результативності впровадження штучного інтелекту є узгодженість інноваційних процесів та інформаційного забезпечення управлінської діяльності. Затримки на етапах розроблення, випробування та впровадження технологічних рішень можуть обмежувати їх практичну цінність, тоді як недостатня достовірність, актуальність і захищеність даних створюють ризики отримання ненадійних алгоритмічних результатів. У цьому зв'язку особливого значення набуває забезпечення послідовного інформаційно-управлінського циклу, що охоплює отримання й захист даних, їх опрацювання, формування аналітичних результатів, підтримку прийняття рішень та оцінювання наслідків їх реалізації. Організаційна узгодженість зазначених процесів потребує визначення відповідальних суб'єктів, розвитку цифрової інфраструктури та належного контролю за результативністю використання інтелектуальних технологій.

Отже, результати дослідження засвідчують, що підвищення обороноздатності держави в умовах розвитку штучного інтелекту залежить не лише від технологічних можливостей, а й від спроможності системи публічного управління забезпечувати узгодженість організаційних, ресурсних та інформаційних процесів. Запропоновані напрями адаптації зарубіжного досвіду створюють основу для вдосконалення відповідних управлінських механізмів з урахуванням національних оборонних потреб та особливостей функціонування сектору безпеки і оборони України в умовах воєнного стану.

3.2. Проблеми публічного управління використання штучного інтелекту для підвищення обороноздатності України та шляхи їх вирішення

Розвиток штучного інтелекту та його інтеграція в діяльність сектору безпеки і оборони України актуалізують необхідність удосконалення підходів до публічного управління у сфері забезпечення обороноздатності держави. Застосування інтелектуальних технологій відкриває можливості для підвищення оперативності опрацювання інформації, вдосконалення інформаційно-аналітичного забезпечення, раціонального використання ресурсів та підтримки прийняття управлінських рішень. Водночас практична реалізація цих можливостей потребує вирішення комплексу нормативно-правових, організаційних, технологічних, кадрових та етико-правових проблем, пов'язаних із впровадженням і використанням штучного інтелекту в оборонній сфері.

В умовах повномасштабної збройної агресії особливого значення набуває спроможність системи публічного управління забезпечувати своєчасне впровадження інноваційних технологій відповідно до актуальних потреб сектору безпеки і оборони. Динамічність безпекового середовища, ресурсні обмеження та підвищені вимоги до захисту інформації зумовлюють необхідність адаптації традиційних управлінських процедур, удосконалення міжвідомчої координації, чіткого розмежування повноважень і запровадження дієвих механізмів контролю за результатами застосування інтелектуальних систем. За таких обставин результативність використання штучного інтелекту визначається не лише його технологічними можливостями, а й ефективністю організації відповідних управлінських процесів.

Водночас наявність розвиненого цифрового середовища, технологічних компаній та інноваційних розробок сама по собі не гарантує готовності системи публічного управління до комплексного використання штучного інтелекту в оборонній сфері. Важливого значення набувають формування спеціалізованих процедур управління даними, оцінювання надійності та безпечності інтелектуальних систем, забезпечення їх організаційної інтеграції та

встановлення відповідальності за результати застосування. Відтак ключова управлінська проблема полягає у невідповідності між динамікою розвитку технологій штучного інтелекту та спроможністю системи публічного управління забезпечувати їх системне, безпечне й результативне впровадження для підвищення обороноздатності України.

Одним із проблемних аспектів є недостатня узгодженість нормативно-правового та організаційного забезпечення використання штучного інтелекту в оборонній сфері. Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р., визначила загальні засади державної політики у відповідній сфері, зокрема необхідність дотримання верховенства права, основоположних прав і свобод людини та демократичних цінностей [111].

Подальший розвиток нормативно-організаційних засад використання штучного інтелекту в Україні передбачено Планом заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки, затвердженим розпорядженням Кабінету Міністрів України від 9 травня 2025 року № 457-р. Зокрема, пунктом 8 зазначеного Плану передбачено прийняття міжнародних стандартів у сфері штучного інтелекту як національних, серед яких ISO/IEC 42001:2023, що визначає вимоги до системи менеджменту штучного інтелекту. Водночас пунктом 9 передбачено забезпечення використання технологій штучного інтелекту у сфері оборони шляхом здійснення відповідних заходів оборонного планування за участю Міністерства оборони України, Апарату Ради національної безпеки і оборони України, Адміністрації Держспецзв'язку та Фонду розвитку інновацій. Поєднання зазначених напрямів державної політики свідчить про необхідність узгодження процесів упровадження інтелектуальних технологій в оборонній сфері з розвитком організаційних процедур управління, оцінювання ризиків і контролю результативності їх застосування [80].

Визначена проблема полягає не лише в необхідності вдосконалення правового регулювання, а й у визначенні процедур практичної реалізації відповідних вимог. Зокрема, потребують належного управлінського

забезпечення питання розмежування повноважень суб'єктів, відповідальних за розроблення, випробування, впровадження та використання інтелектуальних технологій, встановлення вимог до перевірки їх надійності, організації контролю та визначення відповідальності за прийняті рішення. Відсутність достатньо узгоджених процедур може ускладнювати координацію інноваційних процесів, створювати невизначеність щодо відповідальних суб'єктів і негативно впливати на результативність використання відповідних технологій.

Важливим напрямом оптимізації є вдосконалення нормативно-організаційного забезпечення застосування штучного інтелекту з урахуванням специфіки оборонної діяльності. Йдеться про необхідність визначення управлінських процедур, які регламентуватимуть основні етапи життєвого циклу інтелектуальних систем, встановлюватимуть вимоги до їх оцінювання, передбачатимуть належний людський контроль та забезпечуватимуть можливість встановлення відповідальності за результати використання. При цьому регулювання має враховувати відмінності між допоміжними інформаційно-аналітичними системами та технологіями, результати функціонування яких можуть безпосередньо впливати на прийняття критично важливих оборонних рішень.

Іншим проблемним аспектом є організаційна фрагментарність процесів розвитку та впровадження штучного інтелекту. В умовах участі різних органів державної влади, військових структур, науково-дослідних установ, підприємств оборонної промисловості та приватних технологічних компаній виникає потреба в узгодженні їхніх функцій, інтересів і ресурсних можливостей. Недостатня координація між відповідними суб'єктами здатна призводити до дублювання окремих розробок, ускладнення обміну інформацією, затримок у прийнятті управлінських рішень та обмеження можливостей масштабування результативних технологічних рішень.

У цьому контексті особливого значення набуває забезпечення функціональної узгодженості діяльності суб'єктів публічного управління оборонними інноваціями. Оптимізація відповідних процесів має передбачати

чітке визначення відповідальних суб'єктів, розмежування їхніх повноважень, формування узгоджених процедур взаємодії та забезпечення інформаційного супроводу прийняття рішень. При цьому вдосконалення організаційного забезпечення не обов'язково потребує створення нових державних інституцій, оскільки окремі завдання можуть бути реалізовані шляхом підвищення координаційної спроможності наявних органів і структур сектору безпеки і оборони.

Окрему групу становлять проблеми інформаційно-технологічного забезпечення використання штучного інтелекту. Результативність функціонування інтелектуальних систем безпосередньо залежить від якості, повноти, актуальності та захищеності даних, на основі яких здійснюється їх навчання або формування аналітичних результатів. Використання неповних, застарілих чи навмисно спотворених інформаційних масивів може спричиняти помилкові висновки та створювати додаткові ризики для прийняття управлінських рішень. В оборонній сфері зазначені ризики посилюються можливістю цілеспрямованого інформаційного впливу противника, кібератак і втручання у функціонування цифрових систем.

У публічному управлінні відповідна проблематика охоплює не лише технічний захист інформації, а й організацію управління даними, встановлення вимог до їх достовірності, визначення порядку доступу та забезпечення належного контролю за використанням інформаційних ресурсів. Особливого значення набувають узгодження стандартів обміну даними, забезпечення сумісності цифрових платформ і розвиток захищеної інформаційної інфраструктури. Отже, оптимізація інформаційно-технологічного забезпечення має здійснюватися шляхом поєднання організаційних, нормативних і технологічних інструментів, спрямованих на забезпечення надійності інформаційної основи управлінської діяльності.

Важливою проблемою залишається залежність оборонного сектору від зовнішніх постачальників програмного забезпечення, обчислювальних ресурсів та окремих технологічних компонентів. Використання іноземних технологічних

рішень може сприяти прискоренню впровадження інновацій, однак водночас створює ризики обмеження доступу до критично важливих ресурсів, недостатнього контролю за обробленням інформації та ускладнення супроводження відповідних систем. У зв'язку з цим розвиток національного технологічного потенціалу необхідно розглядати як складову забезпечення стійкості публічного управління обороноздатністю.

Водночас технологічна незалежність не повинна ототожнюватися з повною відмовою від міжнародного співробітництва. Доцільним є формування збалансованого підходу, який передбачає розвиток власних критично важливих спроможностей, підтримку національних розробників, забезпечення технологічної сумісності та диверсифікацію постачальників. В управлінському вимірі такий підхід потребує визначення пріоритетів державної підтримки, оцінювання критичних технологічних залежностей і формування механізмів забезпечення безперервності функціонування оборонних інформаційних систем.

Не менш важливим проблемним аспектом є кадрове забезпечення розвитку та використання штучного інтелекту. Впровадження інтелектуальних технологій потребує не лише фахівців із програмування, аналізу даних і супроводження цифрових систем, а й управлінського персоналу, здатного оцінювати можливості, обмеження та ризики відповідних технологій. Недостатній рівень цифрових компетентностей може призводити як до недовикористання потенціалу інтелектуальних систем, так і до надмірної довіри до результатів їх функціонування без належної перевірки.

Оптимізація кадрового забезпечення має передбачати розвиток диференційованої системи професійної підготовки відповідно до функцій учасників управлінського процесу. Для керівного складу пріоритетними є компетентності щодо використання результатів алгоритмічного аналізу під час прийняття рішень, оцінювання ризиків і визначення відповідальності. Для технічних фахівців важливими залишаються навички розроблення, перевірки, супроводження та захисту інтелектуальних систем. Для безпосередніх користувачів необхідним є розуміння функціональних можливостей технологій,

правил їх безпечного застосування та обмежень достовірності отриманих результатів, що дозволяє пов’язати розвиток кадрового потенціалу з конкретними управлінськими завданнями оборонного сектору.

Особливого значення набувають етико-правові проблеми використання штучного інтелекту, пов’язані із захистом прав людини, забезпеченням належного людського контролю та визначенням відповідальності за результати застосування інтелектуальних систем. Використання технологій автоматизованого аналізу інформації, зокрема біометричних даних, може створювати ризики неправомірного втручання у приватне життя, помилкової ідентифікації осіб і прийняття необґрунтованих рішень. Зазначені ризики потребують особливої уваги у випадках, коли технології, розроблені для виконання оборонних завдань, використовуються також у правоохоронній або іншій діяльності державних органів.

Показовим прикладом практичного використання технологій біометричної ідентифікації є застосування в Україні систем компанії Clearview AI. За повідомленням Reuters, у березні 2022 року Міністерство оборони України розпочало використання відповідної технології розпізнавання облич [174]. Подальше дослідження Бібліотеки Конгресу США засвідчує її застосування українськими державними органами для виконання різних завдань, зокрема ідентифікації осіб та сприяння розслідуванню воєнних злочинів [190]. Водночас використання таких систем актуалізує питання правомірності оброблення біометричних даних, достовірності результатів ідентифікації, розмежування повноважень користувачів та забезпечення належного контролю. З позиції публічного управління зазначений приклад демонструє необхідність поєднання технологічних можливостей із чітко визначеними процедурами їх відповідального застосування.

Важливою умовою забезпечення відповідальності під час використання штучного інтелекту є недопущення підміни управлінського рішення автоматизованим результатом без належного оцінювання його достовірності. Алгоритмічні системи можуть сприяти оперативному опрацюванню інформації

та формуванню аналітичних рекомендацій, однак їхні результати не завжди є повними, достовірними або достатньо пояснюваними. Тому використання інтелектуальних технологій у процесах, пов’язаних із критично важливими оборонними рішеннями, потребує встановлення належного рівня людського контролю, документування підстав прийняття рішень та визначення відповідальності уповноважених осіб.

Необхідність збереження людського контролю над процесами прийняття військових рішень підтверджується дослідженням Міжнародного комітету Червоного Хреста, у якому розглянуто вплив автоматизованих систем підтримки рішень на діяльність військового персоналу. Наголошується, що навіть за відсутності самостійного прийняття рішень такими системами сформовані ними аналітичні результати можуть істотно впливати на оцінювання обставин та подальші дії уповноважених осіб, це актуалізує необхідність забезпечення належної підготовки персоналу, перевірки достовірності алгоритмічних результатів і визначення процедур відповідального використання інтелектуальних технологій [184].

Водночас механізми контролю мають враховувати характер і рівень ризику конкретного застосування штучного інтелекту. Використання інтелектуальних систем для виконання допоміжних адміністративних завдань та їх застосування в процесах, що можуть мати безпосередні наслідки для життя і безпеки людей, потребують різних за інтенсивністю процедур оцінювання й нагляду. У зв’язку з цим перспективним напрямом удосконалення публічного управління є запровадження диференційованого підходу до визначення вимог безпеки, перевірки результатів, людського контролю та відповідальності залежно від функціонального призначення інтелектуальної системи й можливих наслідків її застосування.

Суттєвого значення набуває також проблема узгодження оперативності впровадження оборонних інновацій із вимогами законності, підзвітності та належного контролю. В умовах воєнного стану необхідність швидкого реагування на оборонні потреби може обумовлювати застосування прискорених

організаційних процедур. Однак скорочення строків прийняття рішень не повинно призводити до усунення необхідних перевірок безпеки, невизначеності відповідальності або ігнорування ризиків застосування інтелектуальних технологій. Отже, актуальним управлінським завданням є формування процедур, здатних забезпечувати одночасно оперативність інноваційних процесів і достатній рівень контролю за їх результатами.

У цьому контексті доцільним є використання поетапного підходу до впровадження інтелектуальних технологій, який передбачає визначення оборонної потреби, попереднє оцінювання функціонального призначення системи, перевірку надійності, обмежену апробацію, прийняття рішення щодо подальшого використання та моніторинг результативності. Важливою умовою є забезпечення можливості перегляду відповідного рішення у випадку виявлення нових ризиків, зміни умов застосування або недостатньої ефективності технології. Запропоноване дозволяє розглядати управління впровадженням штучного інтелекту як послідовний процес, у межах якого результати оцінювання використовуються для коригування подальших управлінських дій.

Окремої уваги потребує взаємодія держави з приватним технологічним сектором та науковими установами. Розвиток української оборонно-технологічної екосистеми, зокрема використання інноваційних платформ на кшталт Brave1, створює передумови для залучення розробників до виконання актуальних оборонних завдань. Водночас результативність відповідної співпраці залежить від належного визначення державних технологічних потреб, організації випробувань, забезпечення захисту інформації та встановлення прозорих процедур взаємодії між учасниками. Важливим є не лише стимулювання створення нових технологічних рішень, а й забезпечення їх відповідності практичним потребам оборонного сектору та можливості подальшого використання.

Практичним прикладом розвитку відповідної взаємодії є діяльність кластера оборонних технологій Brave1, серед пріоритетних напрямів якого визначено, зокрема, розроблення та впровадження рішень із використанням

штучного інтелекту [170]. З управлінської позиції функціонування такого інноваційного середовища актуалізує необхідність узгодження державних оборонних потреб із можливостями розробників, забезпечення належної організації випробувань і формування процедур переходу від перспективних технологічних рішень до їх практичного використання.

Проведений аналіз засвідчує взаємопов'язаний характер нормативно-правових, організаційно-координаційних, інформаційно-технологічних, ресурсних, кадрових, етико-правових та інноваційно-процедурних проблем публічного управління використання штучного інтелекту в секторі безпеки і оборони України. Їх виникнення та поглиблення зумовлюються не лише окремими технологічними обмеженнями, а й недостатньою узгодженістю управлінських повноважень, процедур і ресурсного забезпечення. З метою встановлення взаємозв'язку між причинами виявлених проблем, їх управлінськими наслідками та можливими механізмами оптимізації розроблено відповідну матрицю (табл. 3.2).

Таблиця 3.2

Матриця проблем публічного управління використання штучного інтелекту для підвищення обороноздатності України та механізмів їх оптимізації

Група проблем	Основні причини та прояви	Управлінські наслідки	Механізми оптимізації
1. Нормативно-правові	Недостатня конкретизація процедур застосування ШІ в оборонній сфері; невизначеність окремих питань відповідальності та контролю	Неоднозначність управлінських процедур, ризики неправомірних рішень	Диференційовані вимоги до застосування ШІ; регламентація процедур оцінювання, контролю та відповідальності
2. Організаційно-координаційні	Недостатня узгодженість діяльності суб'єктів, розподілу функцій і процедур взаємодії	Дублювання управлінських дій, затримки впровадження, неефективне використання ресурсів	Розмежування повноважень; міжвідомча координація; визначення відповідальних за етапи впровадження

Продовження таблиці 3.2

Група проблем	Основні причини та прояви	Управлінські наслідки	Механізми оптимізації
3. Інформаційно-технологічні	Неоднорідність інформаційних систем, недостатня якість і захищеність даних, ризики кібервтручання	Зниження достовірності алгоритмічних результатів, порушення інформаційного забезпечення	Стандарти управління даними; перевірка їх якості; захищений інформаційний обмін; оцінювання надійності систем
4. Ресурсно-технологічні	Обмеженість фінансових та обчислювальних ресурсів; залежність від окремих зовнішніх постачальників	Ускладнення масштабування технологій, ризики порушення безперервності функціонування систем	Пріоритизація ресурсів; оцінювання технологічних залежностей; підтримка критично важливих національних розробок
5. Кадрово-компетентнісні	Недостатність спеціалізованої підготовки управлінського, військового та технічного персоналу	Помилки використання ШІ, надмірна довіра до алгоритмічних результатів, недостатня результативність технологій	Диференційована професійна підготовка; розвиток цифрових і управлінських компетентностей; оцінювання готовності персоналу
6. Етико-правові та контрольні	Ризики порушення прав людини, помилкової ідентифікації, алгоритмічної упередженості; недостатня визначеність процедур людського контролю	Неправомірні рішення, складність встановлення відповідальності, зниження довіри до технологій	Ризик-орієнтоване оцінювання; людський контроль; документування рішень; процедури перевірки та оскарження, де це застосовано
7. Інноваційно-процедурні	Тривалість погоджень і випробувань; недостатній зворотний зв'язок із користувачами; труднощі переходу від розробки до використання	Затримки впровадження, невідповідність технологій актуальним оборонним потребам	Поетапна апробація; прискорені процедури з необхідними перевірками; моніторинг результативності та коригування рішень

Джерело: власна розробка автора

Представлена в табл. 3.2 матриця засвідчує, що кожна з визначених груп проблем характеризується специфічними причинами виникнення, управлінськими наслідками та можливими механізмами оптимізації. Водночас їх

взаємозалежність обумовлює необхідність формування підходу, який забезпечуватиме не лише встановлення відповідності між окремою проблемою та інструментом її вирішення, а й узгодженість управлінських дій у межах єдиного процесу.

У зв'язку з цим запропоновано проблемно-адаптивний підхід до вдосконалення публічного управління використання штучного інтелекту для підвищення обороноздатності України, визначальною особливістю якого є поєднання проблемно орієнтованого добору управлінських механізмів із можливістю їх коригування відповідно до змін оборонних потреб, ресурсних можливостей і безпекового середовища.

Методологічним підґрунтям удосконалення управлінських процедур у сфері штучного інтелекту можуть слугувати міжнародні підходи до управління ризиками та організаційного забезпечення використання відповідних технологій. Зокрема, рамкова модель NIST AI RMF 1.0 передбачає взаємопов'язане здійснення функцій управління ризиками, що охоплюють формування управлінських засад, визначення контексту, оцінювання та реагування на ризики штучного інтелекту [218]. Водночас міжнародний стандарт ISO/IEC 42001:2023 визначає вимоги до створення, впровадження, підтримання та постійного вдосконалення системи менеджменту штучного інтелекту в організаціях [185]. Урахування зазначених положень у межах запропонованого проблемно-адаптивного підходу дозволяє посилити його методологічну обґрунтованість, зберігаючи спрямованість на вирішення специфічних проблем публічного управління використання штучного інтелекту для підвищення обороноздатності України.

Реалізація зазначеного підходу передбачає п'ять взаємопов'язаних етапів. На першому етапі здійснюється виявлення та систематизація проблем, які обмежують результативність розвитку й використання інтелектуальних технологій. Другий етап охоплює оцінювання їх критичності, взаємозалежності та впливу на виконання оборонних завдань, що дозволяє визначити пріоритетність управлінського реагування. На третьому етапі здійснюється добір

відповідних механізмів оптимізації з урахуванням характеру проблем, функціональних повноважень суб'єктів управління та наявних ресурсів. Четвертий етап передбачає організацію реалізації управлінських рішень, визначення відповідальних суб'єктів, необхідних ресурсів, строків і процедур контролю. П'ятий етап охоплює моніторинг отриманих результатів, оцінювання ефективності застосованих механізмів і коригування управлінських рішень за необхідності.

Важливою характеристикою запропонованого підходу є його адаптивність, що проявляється в можливості перегляду пріоритетів і механізмів управлінського впливу залежно від змін безпекового середовища та фактичних результатів використання штучного інтелекту. При цьому оцінювання результативності не обмежується завершальним етапом, а забезпечує зворотний зв'язок із попередніми етапами управлінського процесу. Зазначене створює передумови для своєчасного виявлення нових проблем, уточнення причин їх виникнення та вдосконалення застосованих управлінських інструментів.

Застосування запропонованого підходу може сприяти підвищенню обґрунтованості управлінських рішень, зменшенню організаційної фрагментарності, раціональнішому використанню ресурсів, удосконаленню контролю за впровадженням інтелектуальних технологій та посиленню адаптивності системи публічного управління до змін оборонних потреб України.

Визначення пріоритетності управлінських проблем становить важливу складову запропонованого проблемно-адаптивного підходу, оскільки обмеженість ресурсів і необхідність оперативного реагування на зміни безпекового середовища унеможливлюють одночасне застосування однакових за інтенсивністю заходів до всіх виявлених проблем. За таких умов доцільним є використання системи критеріїв, що дозволяє оцінювати не лише характер проблеми, а й ступінь її впливу на обороноздатність, терміновість реагування, масштаб управлінських наслідків, ресурсні можливості та рівень супутніх ризиків.

З огляду на зазначене запропоновано п’ять взаємопов’язаних критеріїв визначення пріоритетності проблем публічного управління використання штучного інтелекту в секторі безпеки і оборони України (табл. 3.3). Їх застосування спрямоване на забезпечення обґрунтованого розподілу управлінської уваги та ресурсів відповідно до характеру виявлених проблем і потенційних наслідків їх невирішення.

Таблиця 3.3

Критерії визначення пріоритетності проблем публічного управління використання штучного інтелекту для підвищення обороноздатності України

Критерій	**Зміст оцінювання**	**Управлінське значення**
Критичність для обороноздатності	Ступінь впливу проблеми на виконання оборонних завдань, безперервність управління та надійність критично важливих систем	Визначення проблем, які потребують першочергового реагування
Терміновість реагування	Можливість поглиблення негативних наслідків у разі відтермінування управлінських заходів	Визначення допустимих строків реагування
Масштаб управлінських наслідків	Кількість залучених суб’єктів, процесів і функцій, на які впливає проблема	Встановлення необхідного рівня міжвідомчої координації
Ресурсна забезпеченість вирішення	Наявність фінансових, кадрових, організаційних і технологічних ресурсів для усунення проблеми	Оцінювання можливості реалізації управлінських заходів
Рівень безпекових і правових ризиків	Імовірність та тяжкість негативних наслідків для безпеки людей, захисту інформації, законності й відповідальності	Визначення необхідної інтенсивності контролю

Джерело: запропоновано автором

Практичне застосування запропонованих критеріїв передбачає послідовне оцінювання виявлених проблем із визначенням їх критичності для обороноздатності, терміновості управлінського реагування та потенційного масштабу наслідків. При цьому проблеми, що створюють безпосередні загрози життю людей, безперервності виконання оборонних завдань або

функціонуванню критично важливих інформаційних систем, мають розглядатися як першочергові незалежно від складності їх ресурсного забезпечення. Для інших проблем пріоритетність визначається з урахуванням співвідношення очікуваних результатів, доступних ресурсів і можливих наслідків відтермінування управлінських заходів, де визначений порядок дозволяє уникнути ситуації, за якої ресурсна доступність окремого рішення стає визначальним чинником на шкоду його оборонній значущості.

Наступним елементом проблемно-адаптивного підходу є диференційований добір управлінських механізмів оптимізації. Його сутність полягає у встановленні відповідності між характером виявленої проблеми, причинами її виникнення, ступенем критичності та інструментами управлінського впливу, застосування яких є організаційно доцільним, нормативно допустимим і ресурсно обґрунтованим.

У межах третього етапу проблемно-адаптивного підходу порядок добору управлінських механізмів конкретизовано через п’ять послідовних кроків, що забезпечують перехід від визначення характеру проблеми до встановлення очікуваних результатів її вирішення. Запропоновано здійснювати добір відповідних механізмів у п’ять послідовних кроків: ідентифікація проблеми та її причин; оцінювання пріоритетності; визначення можливих механізмів управлінського впливу; перевірка їх відповідності умовам реалізації; встановлення очікуваних результатів і показників оцінювання. При цьому для вирішення проблем комплексного характеру передбачається можливість поєднання декількох взаємодоповнювальних механізмів.

Визначальною особливістю такого порядку є відмова від універсального застосування однакових управлінських інструментів до різних за характером проблем. Зокрема, нормативна невизначеність потребує передусім удосконалення регламентації відповідних процедур, організаційна фрагментарність – узгодження повноважень і міжвідомчої взаємодії, кадрові обмеження – розвитку професійних компетентностей, а ризики ненадійності

алгоритмічних результатів – поєднання технічної перевірки, організаційного контролю та відповідальності уповноважених осіб.

Отже, диференційований добір управлінських механізмів дозволяє забезпечити їх функціональну відповідність конкретним проблемам і запобігти нераціональному використанню ресурсів на заходи, які не усувають основних причин управлінських ускладнень.

Важливою умовою реалізації запропонованого підходу є узгодження управлінських механізмів у випадках, коли виявлена проблема має комплексний характер. Наприклад, недостатня надійність результатів інтелектуальної системи може бути пов’язана одночасно з низькою якістю вихідних даних, обмеженими компетентностями персоналу та недосконалістю процедур перевірки. За таких обставин застосування виключно технологічних засобів не забезпечуватиме усунення всіх причин проблеми. Доцільним є поєднання заходів управління даними, професійної підготовки, організаційного контролю та визначення відповідальності, що дозволяє спрямовувати управлінський вплив не лише на окремі прояви проблеми, а й на взаємопов’язані чинники її виникнення.

Завершальним елементом проблемно-адаптивного підходу є оцінювання результативності застосованих управлінських механізмів. Його призначення полягає у встановленні ступеня досягнення визначених цілей, своєчасному виявленні відхилень від очікуваних результатів та формуванні підстав для коригування подальших управлінських дій (табл. 3.4).

Таблиця 3.4

Показники оцінювання результативності механізмів оптимізації публічного управління використання штучного інтелекту в оборонній сфері

Напрям оцінювання	**Запропоновані показники**	**Очікуваний результат**
Організаційна координація	Тривалість погодження рішень; кількість неврегульованих випадків дублювання функцій	Скорочення затримок, підвищення узгодженості діяльності
Впровадження технологій	Тривалість переходу від апробації до рішення про застосування; частка систем, що пройшли встановлені перевірки	Оперативніше та обґрунтованіше впровадження

Продовження таблиці 3.4

Напрям оцінювання	**Запропоновані показники**	**Очікуваний результат**
Інформаційна надійність	Частота виявлених критичних помилок; кількість інцидентів порушення цілісності даних	Підвищення надійності інформаційного забезпечення
Ресурсне забезпечення	Відхилення фактичних витрат від планових; частка критичних залежностей, для яких передбачено альтернативні рішення	Раціональніше використання ресурсів і підвищення стійкості
Кадрова спроможність	Частка персоналу, який пройшов підготовку та підтвердив необхідні компетентності	Підвищення готовності персоналу до використання ШІ
Управління ризиками	Частка високоризикових систем із проведеним оцінюванням; кількість невиконаних критичних коригувальних заходів	Зниження неврегульованих ризиків
Управлінська адаптивність	Час реагування на виявлені проблеми; частка виконаних у встановлений строк коригувальних заходів	Своєчасне коригування управлінських рішень

Джерело: запропоновано автором

З метою забезпечення об’єктивності такого оцінювання запропоновано систему показників, згрупованих за напрямами організаційної координації, впровадження технологій, інформаційної надійності, ресурсного забезпечення, кадрової спроможності, управління ризиками та управлінської адаптивності (табл. 3.4). Зазначені показники дозволяють оцінювати не лише факт реалізації управлінських заходів, а й зміни у функціонуванні відповідних процесів.

Особливістю запропонованої системи є поєднання показників оперативності, організаційної узгодженості, надійності, ресурсної обґрунтованості та безпеки використання інтелектуальних технологій. При цьому позитивна динаміка окремого показника не повинна розглядатися як достатня підстава для висновку про загальну результативність управлінського механізму. Зокрема, скорочення строків упровадження технології не може вважатися позитивним результатом, якщо воно супроводжується порушенням необхідних процедур перевірки її надійності або підвищенням рівня неприйнятних ризиків.

Підставами для коригування управлінських рішень у межах проблемно-адаптивного підходу можуть виступати невідповідність фактичних результатів визначеним цілям, виникнення нових безпекових або технологічних ризиків, зміна пріоритетності оборонних потреб, перевищення встановлених ресурсних обмежень чи виявлення недоліків у взаємодії відповідальних суб'єктів. Залежно від характеру встановлених відхилень коригування може передбачати зміну строків і послідовності заходів, перерозподіл ресурсів, уточнення відповідальності або перегляд обраного управлінського механізму. Якщо виявлені відхилення свідчать про неприйнятний рівень ризику, має розглядатися питання про обмеження чи призупинення відповідного застосування технології до усунення критичних недоліків.

Результати оцінювання мають використовуватися для визначення необхідності продовження, зміни або припинення застосування окремих управлінських заходів, перегляду ресурсного забезпечення та уточнення пріоритетів. Отже, моніторинг результативності забезпечує зворотний зв'язок між етапами проблемно-адаптивного підходу та формує основу для його практичної реалізації в умовах змінного безпекового середовища.

Проведене дослідження дозволило обґрунтувати проблемно-адаптивний підхід до вдосконалення публічного управління використання штучного інтелекту для підвищення обороноздатності України, що поєднує систематизацію управлінських проблем, визначення їх пріоритетності, диференційований добір механізмів оптимізації та оцінювання результативності їх застосування. На відміну від відокремленого вирішення нормативних, організаційних, технологічних та інших проблем, запропонований підхід передбачає врахування їх взаємозалежності й забезпечення зворотного зв'язку між етапами управлінського процесу. Його застосування створює передумови для підвищення обґрунтованості управлінських рішень, узгодженості діяльності суб'єктів сектору безпеки і оборони, раціонального використання ресурсів та своєчасного реагування на зміни оборонних потреб і безпекового середовища.

Висновки до розділу 3.

За результатами дослідження зарубіжного досвіду публічного управління використання штучного інтелекту для підвищення обороноздатності держави встановлено, що результативність упровадження інтелектуальних технологій визначається не лише рівнем технологічного розвитку, а й особливостями стратегічного планування, інституційної координації, ресурсного забезпечення, партнерської взаємодії та управління ризиками. На основі порівняльного аналізу практики Австралії, Великої Британії, Франції, Японії та Ізраїлю за критерієм домінантного управлінського пріоритету систематизовано п’ять підходів до публічного управління використання штучного інтелекту в оборонній сфері: стратегічно-координаційний, інституційно-організаційний, централізовано-інституційний, ресурсно-адаптивний та партнерсько-інноваційний.

На підставі отриманих результатів обґрунтовано шість взаємопов’язаних напрямів вибіркової адаптації зарубіжного досвіду до потреб України, що охоплюють удосконалення організаційної координації, розвиток механізмів апробації та впровадження інтелектуальних технологій, формування кадрового й організаційного потенціалу, посилення взаємодії держави з науковим середовищем і приватним сектором, удосконалення процедур управління ризиками та забезпечення технологічної стійкості. Доведено доцільність диференційованого використання відповідних управлінських механізмів з урахуванням національних оборонних пріоритетів, інституційних і ресурсних можливостей, а також особливостей функціонування сектору безпеки і оборони України в умовах воєнного стану.

За результатами дослідження встановлено, що використання штучного інтелекту для підвищення обороноздатності України супроводжується комплексом взаємопов’язаних проблем публічного управління, серед яких виокремлено нормативно-правові, організаційно-координаційні, інформаційно-технологічні, ресурсно-технологічні, кадрово-компетентнісні, етико-правові та контрольні, інноваційно-процедурні. Обґрунтовано, що їх вирішення потребує узгодженого застосування управлінських механізмів, орієнтованих на усунення

причин виникнення проблем, забезпечення міжвідомчої взаємодії, раціонального використання ресурсів та належного контролю за впровадженням інтелектуальних технологій.

Розроблено матрицю проблем публічного управління використання штучного інтелекту та механізмів їх оптимізації, що дозволило встановити взаємозв'язок між причинами виникнення проблем, їх управлінськими наслідками та можливими способами вирішення. На її основі запропоновано проблемно-адаптивний підхід, який передбачає п'ять взаємопов'язаних етапів: виявлення та систематизацію проблем; оцінювання їх пріоритетності; диференційований добір управлінських механізмів; організацію реалізації відповідних рішень; моніторинг результативності та коригування управлінських дій.

Конкретизовано критерії визначення пріоритетності управлінських проблем, що охоплюють їх критичність для обороноздатності, терміновість реагування, масштаб управлінських наслідків, ресурсну забезпеченість вирішення та рівень безпекових і правових ризиків. Запропоновано порядок добору механізмів оптимізації залежно від характеру виявлених проблем і систему показників оцінювання результативності за напрямами організаційної координації, впровадження технологій, інформаційної надійності, ресурсного забезпечення, кадрової спроможності, управління ризиками та управлінської адаптивності.

Обґрунтовано, що застосування проблемно-адаптивного підходу створює передумови для забезпечення послідовності й функціональної узгодженості управлінських дій, своєчасного перегляду пріоритетів, підвищення обґрунтованості управлінських рішень і вдосконалення механізмів використання штучного інтелекту відповідно до змін оборонних потреб, ресурсних можливостей та безпекових умов України.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення і наведено шляхи вирішення наукової проблеми, що полягає у розробленні та обґрунтуванні теоретичних і науково-методологічних підходів щодо використання штучного інтелекту в системі публічного управління для підвищення обороноздатності України. Результати проведеного дослідження дають підстави для формулювання таких ключових теоретичних висновків і практичних рекомендацій:

1. Використання історичного та компаративного методу дозволило виокремити зарубіжні та вітчизняні наукові підходи до визначення сутності штучного інтелекту, його теоретичного розуміння. Уточнено його співвідношення із суміжними технологічними категоріями та конкретизовано технологічні, функціональні та системні характеристики. Доведено, що штучний інтелект перетворюється з суто технологічного інструменту на універсальний, який підсилює інституційну спроможність держави, завдяки здатності оперативно опрацьовувати великі масиви інформації, забезпечувати ефективність планування надаючи можливість прогнозування ризиків, створюючи нові можливості для координації взаємодії органів влади, органів публічної влади надаючи, інноваційні інструменти контролю. Встановлено, що ШІ може функціонувати з різним ступенем автономності, формулювати рекомендації, рішення відповідно до визначених цілей. Сучасний етап розвитку штучного інтелекту в Україні характеризується посиленням його стратегічного значення для цифрової трансформації держави, модернізації публічного управління, розвитку інноваційної економіки та зміцнення національної безпеки й обороноздатності.

2. Обґрунтовано, що визначальними ознаками сучасного штучного інтелекту є здатність до обчислювального висновування на основі даних та/або формалізованих знань, формування прогнозів, рекомендацій, рішень та інших результатів відповідно до визначених цілей, а також функціонування з різним ступенем автономності. Доведено доцільність розгляду штучного інтелекту в

контексті публічного управління як інструменту інформаційно-аналітичного забезпечення, прогнозування та підтримки прийняття управлінських рішень.

3. Розкрито сутність обороноздатності держави як комплексного об'єкта публічного управління в системі національної безпеки, забезпечення якого ґрунтується на взаємодії військових, економічних, технологічних, інформаційних, кадрових та організаційно-управлінських складових. На основі аналізу історичного розвитку обороноздатності України виокремлено п'ять етапів її становлення, що відображають трансформацію публічно-управлінських підходів від формування нормативно-інституційних засад оборони до комплексного й адаптивного управління оборонними ресурсами та спроможностями.

4. Уточнено категорію «забезпечення обороноздатності держави», яку доцільно розглядати як безперервний процес цілеспрямованої діяльності уповноважених суб'єктів, спрямований на формування, підтримання, розвиток і реалізацію оборонного потенціалу та оборонних спроможностей відповідно до визначених цілей державної політики у сфері національної безпеки й оборони. Зазначений процес охоплює стратегічне планування, прогнозування загроз, визначення потреб, ресурсне забезпечення, організацію взаємодії, реалізацію управлінських рішень, моніторинг результатів та коригування заходів відповідно до змін безпекового середовища, що відповідає етапам процесу публічного управління. Встановлено, що поняття «оборона», «обороноздатність», «оборонний потенціал», «оборонні спроможності» та «забезпечення обороноздатності» перебувають у тісному взаємозв'язку, проте не є тотожними. Їх розмежування дозволяє визначити місце публічного управління у формуванні обороноздатності держави.

5. Обґрунтовано інтегрувальну роль публічно-управлінського узгодження у процесі перетворення оборонного потенціалу на оборонні спроможності та запропоновано концептуальну модель забезпечення обороноздатності держави, яка передбачає взаємозв'язок оцінювання безпекових загроз, визначення оборонних потреб, мобілізації ресурсів, координації діяльності суб'єктів,

розвитку оборонних спроможностей і адаптивного коригування управлінських рішень на основі зворотного зв’язку.

6. Систематизовано теоретичні підходи до використання штучного інтелекту в системі публічного управління сектором безпеки і оборони, що дозволило виокремити інструментальний, аналітико-прогностичний, інституційно-управлінський, ризик-орієнтований та адаптивний підходи. На їх основі обґрунтовано п’ять взаємопов’язаних функціональних напрямів застосування штучного інтелекту в публічному управлінні забезпечення обороноздатності держави: інформаційно-аналітичний, прогностичний, планувально-ресурсний, координаційний та контрольно-моніторинговий. Встановлено, що використання ШІ за зазначеними напрямами може сприяти підвищенню якості управлінських рішень, удосконаленню оборонного планування, узгодженню діяльності суб’єктів управління та раціональному використанню оборонних ресурсів.

7. Обґрунтовано, що вплив ШІ на підвищення обороноздатності держави реалізується опосередковано, через посилення управлінської спроможності, удосконалення процесів формування й розвитку обороноздатності за умов належного інституційного забезпечення, управління ризиками, людського контролю та відповідальності за прийняття управлінських рішень.

Запропоноване узагальнення дозволяє розглядати його використання як складову публічно-управлінського забезпечення обороноздатності держави, що спрямована на підвищення обґрунтованості управлінських рішень, удосконалення оборонного планування, узгодження ресурсного забезпечення та розвиток оборонних спроможностей.

8. Досліджено нормативно-правову базу використання ШІ для посилення обороноздатності України, що дозволило зробити висновок про те, що стратегічні й програмні документи створюють загальну політичну основу для розвитку технологій штучного інтелекту та визначають його одним із пріоритетних напрямів. Водночас вони мають переважно декларативний характер і не встановлюють юридично обов’язкових вимог до розроблення та

застосування оборонних ШІ-систем. Відсутність спеціалізованого закону або галузевої стратегії застосування штучного інтелекту в оборонній сфері свідчить про наявність системної прогалини в законодавстві. Зокрема, залишаються законодавчо не врегульованими поняття «автономні системи озброєння», рівні людського контролю та «критичні функції» зброї, що ускладнює формування технічних вимог, укладення договорів і встановлення правомірності їх використання. Разом з тим потрібно не допустити бюрократичні затримки у впровадженні систем штучного інтелекту в оборонну сферу особливо в умовах військових викликів.

9. Встановлено, що нині відбувається процес підготовки Проєкту Закону України «Про правове регулювання штучного інтелекту», а також гармонізація вітчизняного законодавства з міжнародними стандартами. Визначено першочергові заходи для покращення та вдосконалення нормативно-правових засад впровадження штучного інтелекту в секторі безпеки і оборони України. Особливу увагу варто звернути на правове регулювання систем штучного інтелекту, призначених виключно для військових цілей, оборони та забезпечення національної безпеки.

Рекомендовано уточнити понятійно-категоріальний апарат, а саме: закріпити поняття штучного інтелекту, автономних і напівавтономних систем озброєння, а також рівнів людського контролю, узгодивши їх із міжнародною термінологією.

Запропоновано розробити та затвердити галузеву концепцію чи стратегію застосування ШІ у секторі безпеки й оборони, яка включає принципи законності, відповідальності, пояснюваності, надійності, керованості та зменшення упередженості, а також запровадити механізм правової оцінки нових засобів і методів ведення війни, зокрема, систем штучного інтелекту, визначити уповноважений орган і критерії здійснення такого аналізу.

10. Визначено, що суб’єкти публічного управління у сфері забезпечення обороноздатності взаємодіють між собою по вертикалі та по горизонталі, у відповідності до статусу у суспільстві, міри підпорядкування, функціональних

обов’язків та повноважень, які вони виконують. При цьому вертикальні зв’язки відображають відносини підпорядкованості, нормотворення та стратегічного контролю, а горизонтальні – оперативну координацію, обмін даними, спільну R&D-діяльність та міжвідомчу синергію.

11. Запропоновано розглядати інституційну архітектуру публічного управління забезпечення ШІ у сфері обороноздатності України за допомогою п’яти взаємопов’язаних функціональних блоків: політико-законодавчий блок; виконавчо-координаційний блок; безпеково-інфраструктурний блок; оперативно-застосовний блок; інноваційно-технологічний блок. Зазначено, що інституційна архітектура забезпечення ШІ у сфері обороноздатності України була б не повною без освітнього компоненту, оскільки він забезпечує підготовку військових операторів, аналітиків ШІ, розробників оборонних програмних продуктів, інженерів, а також фахівців у сфері публічного управління та адміністрування, які відповідають за забезпечення та регулювання процесів впровадження штучного інтелекту в обороноздатність держави.

12. Узагальнено зарубіжний досвід публічного управління використання штучного інтелекту для підвищення обороноздатності держави. Встановлено, що відмінності зарубіжних практик використання штучного інтелекту в оборонній сфері визначаються не лише рівнем технологічного розвитку держави, а й особливостями організації публічного управління відповідними процесами. В результаті систематизовано п’ять домінантних управлінських підходів: стратегічно-координаційний, інституційно-організаційний, централізовано-інституційний, ресурсно-адаптивний і партнерсько-інноваційний. Встановлено, що їхні відмінності визначаються особливостями стратегічної координації, інституційної організації, ресурсного забезпечення та взаємодії суб’єктів оборонно-інноваційної діяльності. Обґрунтовано шість напрямів вибіркової адаптації зарубіжного досвіду до потреб України, спрямованих на вдосконалення організаційної координації, процедур апробації та впровадження ШІ, кадрового забезпечення, партнерської взаємодії, управління ризиками й технологічної стійкості. Визначено, що їх реалізація має ґрунтуватися на

функціональній доцільності, відповідності національним оборонним пріоритетам та врахуванні інституційних, ресурсних і безпекових умов функціонування сектору безпеки і оборони України.

13. Систематизовано основні проблеми публічного управління, що стосуються використання штучного інтелекту для підвищення обороноздатності України та встановлено їх взаємопов'язаний характер. Удосконалено науково-методичний підхід до оптимізації відповідних управлінських процесів шляхом розроблення матриці проблем і механізмів їх вирішення, визначення критеріїв пріоритетності управлінського реагування, диференційованого добору механізмів оптимізації та системи показників оцінювання результативності.

Важливою характеристикою запропонованого підходу є його адаптивність, що проявляється в можливості перегляду пріоритетів і механізмів управлінського впливу залежно від змін безпекового середовища та фактичних результатів використання штучного інтелекту. При цьому оцінювання результативності не обмежується завершальним етапом, а забезпечує зворотний зв'язок із попередніми етапами управлінського процесу. Зазначене створює передумови для своєчасного виявлення нових проблем, уточнення причин їх виникнення та вдосконалення застосованих управлінських інструментів.

Застосування запропонованого підходу може сприяти підвищенню обґрунтованості управлінських рішень, зменшенню організаційної фрагментарності, раціональнішому використанню ресурсів, удосконаленню контролю за впровадженням інтелектуальних технологій та посиленню адаптивності системи публічного управління до змін оборонних потреб України.

Все це складає основу проблемно-адаптивного підходу, який забезпечує узгодження управлінських дій, раціональне використання ресурсів і своєчасне коригування рішень відповідно до змін оборонних потреб та безпекового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Автоматизація реагування на інциденти (рішення SOAR). URL: https://www.seeton.pro/cybersecurity/soar/.

2. Алюшина Н. О., Бондар Т. В., Бурдін Я. Є. та ін. Дослідження організаційної культури публічної служби України (2023 рік) : аналітичний звіт. Київ : НАДС, 2023. URL: https://nads.gov.ua/storage/app/sites/5/DIYALNIST/UPRAVLINJA%20PERSONALOM/Analitika%20ta%20doslidgenja/analitichniizvitorganizatsiinakultura2023.pdf.

3. Аналітичний звіт щодо дослідження організаційної культури «Публічна служба в Україні: ваша точка зору». Національне агентство України з питань державної служби. 2025. URL: https://nads.gov.ua/storage/app/sites/5/uploaded-files/analiticnii-zvit.pdf.

4. Амосов М. М. Штучний розум. Київ : Наукова думка, 1969. URL: https://www.icfcst.kiev.ua/amosov/nature.

5. Аналіз секторального напряму та первинне бачення розвитку сфери ШІ. Міністерство цифрової трансформації України. URL: https://winwin.gov.ua/assets/files/%D0%A3%D0%9A%D0%A0%20WINWIN_AI_1.pdf.

6. Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право*. 2023. № 1 (44). С. 32–49. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287537.

7. Берназюк І. М. Рамкова Конвенція Ради Європи про штучний інтелект у контексті захисту прав людини: виклики та значення для України європейського Акта про ШІ / AI Act. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2026. Том 3, № 93. С. 18-30. DOI: https://doi.org/10.24144/2307-3322.2026.93.3.2.

8. Бєлай С. В., Споришев К. О. Системи підтримки прийняття рішень у державному управлінні силами безпеки України. *Актуальні питання у сучасній науці* (Серія «Державне управління»). 2024. Вип. № 2(20). С. 320–329.

9. Біла книга з регулювання штучного інтелекту в Україні: бачення

Мінцифри. Міністерство цифрової трансформації України. Київ, 2024. URL: https://thedigital.gov.ua.

10. Богданович В. Ю., Свида І. Ю., Скулиш Є. Д. Теоретико-методологічні основи забезпечення національної безпеки України : монографія. Воєнна безпека держави і шляхи її забезпечення. За заг. ред. Є. Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. Т. 4. 464 с.

11. Богданович В., Троцько В., Цибуленко М. Оборонна достатність держави (умови для обґрунтування достатнього рівня). *Військо України*. 1997. № 3–4. С. 6–7.

12. Богуцький П. П. Публічне адміністрування у сфері оборони України: телеологія воєнної безпеки. *Право України*. 2024. № 8. С. 71–82. DOI: https://doi.org/10.33498/louu-2024-08-071.

13. Брайлян Є. Ефективні дії ЗСУ на великій війні спонукали НАТО до покращення командування й розвідки в Альянсі. 2023. URL: https://armyinform.com.ua/2023/03/21/efektyvni-diyi-zsu-na-velykij-vijni-sponukaly-nato-do-pokrashhennya-komanduvannya-j-rozvidky-v-alyansi/.

14. Бучинська А. Й. Нормативне регулювання штучного інтелекту в Європейському Союзі: етапи, виклики, перспективи. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. Випуск № 03. С.259-265. DOI : https://doi.org/10.24144/2788-6018.2025.03.3.40.

15. В українських університетах створюватимуть дослідницькі лабораторії зі штучного інтелекту. Міністерство цифрової трансформації України. 2020. URL: https://thedigital.gov.ua/news/education/v-ukrainskikh-universitetakh-stvoryuvatimut-doslidnitski-laboratorii-zi-shtuchnogo-intelektu.

16. Василенко В. М. Інтеграція систем штучного інтелекту в державне управління: ризики, правові виклики та безпекові гарантії. Вісник кримінологічної асоціації України. 2025. №2 (35). Частина 2. С. 574-585. DOI: https://doi.org/10.32631/vca.2025.2.82.

17. Використання ШІ в публічному управлінні: від технологічного тренду до практичних рішень. Національне агентство України з питань державної

служби. 2026. URL: https://nads.gov.ua/news/vykorystannia-shi-v-publichnomu-upravlinni-vid-tekhnolohichnoho-trendu-dopraktychnykh-rishen.

18. Військова академія м. Одеса. Офіційний сайт. https://vaodesa.mil.gov.ua/.·

19. Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. Офіційний сайт. https://mitit.mil.gov.ua/. ·

20. Вольська О. М. Особливості державної політики національної безпеки крізь призму сутності, структурних характеристик та параметрів функціонування. *Публічне адміністрування та національна безпека*. 2025. № 11 (64). С. 59–65. DOI: https://doi.org/10.25313/2617-572X-2025-11-11663.

21. Вольська О. Публічно-управлінський інструментарій використання ШІ органами державної влади у сфері оборони. *Вісник Хмельницького національного університет*. Серія: Економічні науки. 2026. № 4. С. 383-388. DOI: https://doi.org/10.31891/2307-5740-2026-356-51.

22. Гайдамашко О. Україна готує закон про ШІ: які правила та заборони чекають на розробників штучного інтелекту. 24 канал. URL : https://24tv.ua/tech/zakon-pro-shtuchniy-intelekt-ukrayini-vzhe-znahoditsya-rozrobtsi_n3138282.

23. Гачкевич А. О. До питання правової визначеності поняття штучного інтелекту. *Вісник Національної академії правових наук України*. 2025. Т. 32, № 1. С. 27–46. DOI: https://doi.org/10.31359/1993-0909-2025-32-1-27.

24. Глушков В. М. Енциклопедія Сучасної України. URL: https://esu.com.ua/article-30542.

25. Гончаренко Г. А. Управління сектором безпеки: поняття й сутність. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: юридичні науки. 2020. Том 31 (70) Ч. 2 № 2. DOI https://doi.org/10.32838/2707-0581/2020.2-2/08.

26. Даник Ю., Дикий А., Шестаков В., Ширшов Р. Аналіз та обґрунтування запровадження і використання штучного інтелекту для потреб сектору безпеки та оборони України. *Society and Security*, № 6(12), 2025. С. 64–76. URL : https://doi.org/10.26642/sas-2025-6(12)-64-76.

27. Декларація про державний суверенітет України : Декларація Верховної Ради УРСР від 16.07.1990 № 55-XII. URL: https://zakon.rada.gov.ua/laws/show/55-12.

28. Демидова Л. М. Обороноздатність України як об'єкт кримінально-правової охорони. *Юридичний науковий електронний журнал*. 2024. № 10, С.364-366. DOI : https://doi.org/10.32782/2524-0374/2024-10/84.

29. До 90% швидше: як ШІ змінює виявлення та ураження цілей у Силах оборони. АрміяInform. 2026. URL: https://armyinform.com.ua/2026/08/28/do-90-shvydshe-yak-shi-zminyuye-vyyavlennya-ta-urazhennya-czilej-u-sylah-oborony/.

30. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. Документ 995_199, чинний. Редакція від 08.12.2005. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text.

31. Дорожня карта з регулювання штучного інтелекту в Україні. Міністерство цифрової трансформації України. Київ, 2023. URL: https://thedigital.gov.ua.

32. Духневич О. В. Концептуальні підходи до стратегічного прогнозування у публічному управлінні. *Ефективність державного управління*. 2025. № 1(82/83), С. 53–60. DOI: https://doi.org/10.36930/508207.

33. Забокрицький І. І. Акт про штучний інтелект (Artifical Inteligence Act, AI ACT) як основа правового регулювання штучного інтелекту в ЄС: огляд основних положень. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. Том 3 № 3. С. 282-286. DOI: https://doi.org/10.24144/2788-6018.2025.03.3.44.

34. Звіт про результати публічного громадського обговорення проекту розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку сфери штучного інтелекту в Україні на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2026-2028 роках». Міністерство цифрової трансформації України. URL: https://storage.thedigital.gov.ua/files/d/fd/de554aec53edacb8f8143015ea6f8fd2.pdf.

35. ЗСУ затвердили Концепцію використання штучного інтелекту. Fintech Insider. 2024. URL: https://fintechinsider.com.ua/zsu-zatverdyly-konczepcziyu-vykorystannya-shtuchnogo-intelektu/.

36. Івахненко О. Г. До 100-річчя академіка. КПІ ім. Ігоря Сікорського. URL: https://kpi.ua/ivakhnenko-about.

37. Інститут проблем штучного інтелекту. Історія ІПШІ. URL: https://www.ipai.net.ua/uk/istoriya-ipshi.

38. Карпенко О. В., Карпенко Ю. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. *Державне управління: удосконалення та розвиток*. 2021. № 10. DOI: https://doi.org/10.32702/2307-2156-2021.10.2.

39. Кластер оборонних технологій BRAVE1 : офіційний вебсайт. URL: https://brave1.gov.ua/.

40. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

41. Концепція Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року. Схвалено розпорядженням Кабінету Міністрів України від 13 квітня 2024 р. № 320-р URL: https://osvita.ua/doc/files/news/918/91892/661ab241436cc732884172.pdf.

42. Концепція розвитку штучного інтелекту в Україні. Документ 1556-2020-р, чинний. Редакція від 29.12.2021. URL : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

43. Костенко О. М. Штучний інтелект: погляд крізь оптику соціального натуралізму. *Вісник Національної академії наук України*. 2026. № 8. С. 3–11. DOI: https://doi.org/10.15407/visn2026.08.003.

44. Котляренко О. П. Характеристика змісту та обсягу повноважень Президента України як Верховного Головнокомандувача Збройних Сил України. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2022,

№2. С. 52-58. DOI : https://doi.org/10.24144/2788-6018.2022.02.9.

45. Куцій І. М. Мотивація державних службовців як наукова категорія публічного управління: теоретичні підходи та концептуальні основи. *Таврійський науковий вісник.* Серія Публічне управління та адміністрування. 2026. № 4. С. 50-60. DOI : https://doi.org/10.32782/tnv-pub.2026.4.6.

46. Магиляс Ю., Корсун В., Миргородська М. Пріоритетні напрямки впровадження штучного інтелекту в публічне управління. *Аспекти публічного управління*. 2023. Вип. 11 (4). С. 97–103. DOI: https://doi.org/10.15421/152358.

47. Мартинов А. Ю. Партнерство заради миру. *Енциклопедія Сучасної України*. 2024. URL: https://esu.com.ua/article-883847.

48. Мартинюк А. І. Розбудова публічного управління в умовах воєнного стану в україні: аналіз комплексу безпекових викликів. *Публічне урядування*. 2026. Випуск 2 (47). С. 62-72. DOI : https://doi.org/10.32689/3083-774X-2026-2(47)-8.

49. Мартинюк Р. С., Дацюк О. Президент України у сфері забезпечення національної безпеки та обороноздатності держави. Часопис Національного університету «Острозька академія». Серія «Право». 2021, № 1(23). URL: https://eprints.oa.edu.ua/id/eprint/10321/.

50. Мачуський В. В., Мачуська І. Б., Тітова В .М., Тітова О. С., Мачуський В. В. Біла книга зі штучного інтелекту як джерело формування законодавства Європейського Союзу у сфері штучного інтелекту. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 2. С. 226-230. DOI: https://doi.org/10.24144/2788-6018.2024.02.39.

51. Меморандум про гарантії безпеки у зв’язку з приєднанням України до Договору про нерозповсюдження ядерної зброї : Меморандум від 05.12.1994. URL: https://zakon.rada.gov.ua/laws/show/998_158.

52. Менше рутини у штабах: ШІ-платформа SPECTR аналізуватиме бойові дані та прогнозуватиме дії противника. Міністерство оборони України. 2026. URL: https://mod.gov.ua/news/menshe-rutyny-u-shtabakh-shi-platforma-spectr-analizuvatyme-boiovi-dani-ta-prohnozuvatyme-dii-protyvnyka.

53. Мінцифри запускає центр передового досвіду з розробки та інтеграції ШІ. Кабінет Міністрів України. 04.02.2025. URL: https://www.kmu.gov.ua/news/mintsyfry-zapuskaie-tsentr-peredovoho-dosvidu-z-rozrobky-ta-intehratsii-shi.

54. Науково-практичний коментар Кримінального кодексу України /за ред. М. І. Мельника, М. І. Хавронюка. 9-те вид., переробл та допов. Київ: Юридична думка, 2012. 1316 с.

55. Національний університет оборони України. Офіційний сайт. https://nuou.org.ua/.

56. Некряч А. І. Державне управління використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищенні обороноздатності України. *Український журнал прикладної економіки та техніки*. 2026. Т. 11, № 3. С. 331–336. DOI: https://doi.org/10.36887/2415-8453-2026-3-59.

57. Некряч А., Дабіжа В. Обороноздатність держави як об’єкт публічного управління в умовах стрімкого розвитку штучного інтелекту. *Modeling the Development of the Economic Systems*. 2026. № 3. С. 364–371. DOI: https://doi.org/10.31891/mdes/2026-21-41.

58. НТУУ «Київський політехнічний інститут імені Ігоря Сікорського». Кафедра штучного інтелекту (ШІ), НН ІПСА. Офіційний сайт. https://kpi.ua/web-ai-iasa.·

59. Організація сектору безпеки і оборони України: навчальний посібник / за заг. ред. д-ра військ. наук, доц. В. В. Овчаренка. Київ: КІНГУ. 2023. 316 с. URL: https://kingu.edu.ua/wp-content/uploads/2024/09/%D0%9E%D0%A1%D0%91%D0%9E.pdf.

60. Пасічко В. Обороноздатність держави: теоретичні основи системного дослідження. *Політичний менеджмент*. 2008. № 2. С. 135-145. URL: http://nbuv.gov.ua/UJRN/PoMe_2008_2_15.

61. Перевалова Л. В., Кузьменко О. В., Григоренко Я. О. Обороноздатність VS воєнна безпека держави: теоретико-правовий аспект. *Вісник Запорізького національного університету*. Юридичні науки. 2019. Вип.1, С. 7-13. URL:

https://repository.kpi.kharkov.ua/ server/api/core/ bitstreams /d15f9d41-6bb9-46da-8f78-ac2587b1ea98/content.

62. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки. Документ 457-2025-р, чинний. Прийняття від 09.05.2025. URL : https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text.

63. Платформа C4ISR: архітектура та компоненти. Corvus Intelligence. 2026. URL : https://corvusintell.com/uk/blog/c2-systems/c4isr-platform-explained/. ·

64. Повідомлення про оприлюднення проєкту розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку штучного інтелекту в Україні на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2026-2028 роках». 2026. URL : https://thedigital.gov.ua/documents/ministry/povidomlennia-pro-opryliudnennia-proyektu-rozporiadzennia-kabinetu-ministriv-ukrayiny-pro-skhvalennia-stratehiyi-rozvytku-shtuchnoho-intelektu-v-ukrayini-na-period-do-2030-roku-ta-zatverdzennia-operatsiynoho-planu-zakhodiv-z-yiyi-realizatsiyi-u-2026-2028-rokakh.

65. Положення про Грантову програму Brave1 EU4UA Defence Tech. Затверджено Рішенням Наглядової ради Фонду розвитку інновацій від 20 листопада 2025 року № 133 (зі змінами від 21 квітня 2026 року № 164). URL : https://files.brave1.gov.ua/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%20%D0%93%D1%80%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%83%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%20Brave1%20EU4UA%20Defence%20Tech.pdf.

66. Положення про Спеціальну грантову програму Brave1 Tech EU. Затверджено Рішенням Наглядової ради Фонду розвитку інновацій від 23 червня 2026 року № 173 (зі змінами від 06 серпня 2026 року № 180). URL : https://files.brave1.gov.ua/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%20%D0%A1%D0%BF%D0%B5%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%83%20%D0%B3%D1%80%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D

1%83%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%20Brave1%20Tech%20EU.pdf.

67. Положення про умови проведення грантового конкурсу Brave1 International NATO. Затверджене: протоколом засідання Наглядової ради Фонду розвитку інновацій від 27 липня 2026 року № 178 (зі змінами від 6 серпня 2026 року № 181). URL : https://files.brave1.gov.ua/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%20%D1%83%D0%BC%D0%BE%D0%B2%D0%B8%20%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%B3%D1%80%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE%20%D0%BA%D0%BE%D0%BD%D0%BA%D1%83%D1%80%D1%81%D1%83%20Brave1%20International%20NATO%20%20Regulations%20on%20the%20Terms%20and%20Conditions%20for%20Conducting%20the%20Brave1%20International%20NATO%20Grant%20Competition.pdf.

68. Пояснювальна записка до проекту розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку штучного інтелекту в Україні на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2026-2028 роках». URL : ttps://storage.thedigital.gov.ua/files/c/cc/1566bb055d364df99a19bcca2eb4ccce.pdf.

69. Права людини в епоху штучного інтелекту: виклики та правове регулювання : методичний матеріал / У. Шадська, А. Ніколаєв, Ю. Деркаченко та ін. ; проєкт EU4DigitalUA. Київ, 2024. 40 с. URL : https://ombudsman.gov.ua/storage/app/media/uploaded-files/%D0%9F%D0%A0%D0%90%D0%92%D0%90%20%D0%9B%D0%AE%D0%94%D0%98%D0%9D%D0%98%20%D0%92%20%D0%95%D0%9F%D0%9E%D0%A5%D0%A3%20%D0%A8%D0%A2%D0%A3%D0%A7%D0%9D%D0%9E%D0%93%D0%9E%20%D0%86%D0%9D%D0%A2%D0%95%D0%9B%D0%95%D0%9A%D0%A2%D0%A3_compressed.pdf.

70. Про авторське право і суміжні права : Закон України від 1 груд. 2022 р.

Документ 2811-IX, чинний. Редакція від 31.07.2026. URL: https://zakon.rada.gov.ua/laws/show/2811-20.

71. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022.

72. Про військовий обов'язок і військову службу : Закон України від 25.03.1992 № 2232-XII. URL: https://zakon.rada.gov.ua/laws/show/2232-12.

73. Про військові формування в Україні : Постанова Верховної Ради Української РСР від 24.08.1991 № 1431-XII. URL: https://zakon.rada.gov.ua/laws/show/1431-12.

74. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави : Закон України від 19.06.2003 № 975-IV. URL: https://zakon.rada.gov.ua/laws/show/975-15.

75. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання : Закон України від 20 лют. 2003 р. Документ 549-IV, чинний. Редакція від 05.10.2025. URL: https://zakon.rada.gov.ua/laws/show/549-15.

76. Про державну допомогу суб'єктам господарювання : Закон України. Документ 1555-VII, чинний. Редакція від 21.06.2026. URL : https://zakon.rada.gov.ua/laws/show/1555-18#Text.

77. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України. Документ 3475-IV, чинний. Редакція від 20.04.2025. URL : https://zakon.rada.gov.ua/laws/show/3475-15#Text.

78. Про державну таємницю : Закон України від 21 січ. 1994 р. Документ 3855-XII, чинний. Редакція від 27.08.2025. URL: https://zakon.rada.gov.ua/laws/show/3855-12.

79. Про електронні комунікації : Закон України. Документ 1089-IX, чинний. Редакція від 30.05.2026. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text.

80. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки : розпорядження Кабінету

Міністрів України від 09.05.2025 № 457-р. URL: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80.

81. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки : розпорядження Кабінету Міністрів України від 12 лют. 2021 р. № 69-р. URL: https://zakon.rada.gov.ua/laws/show/69-2021-р.

82. Про затвердження плану заходів на 2026 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від від 24 червня 2026 р. № 631-р URL: https://zakon.rada.gov.ua/laws/show/631-2026-%D1%80#Text.

83. Про затвердження Положення про Міністерство оборони України : постанова Кабінету Міністрів України від 26 лист. 2014 р. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-п.

84. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. Документ 80/94-ВР, чинний. Редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр.

85. Положення про технічний захист інформації в Україні. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text.

86. Про захист персональних даних : Закон України від 1 черв. 2010 р. Документ 2297-VI, чинний. Редакція від 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

87. Про Збройні Сили України : Закон України від 6 груд. 1991 р. Документ 1934-XII, чинний. Редакція від 28.08.2025. URL: https://zakon.rada.gov.ua/laws/show/1934-12.

88. Про інноваційну діяльність : Закон України. Документ 40-IV, чинний. Редакція від 31.03.2023. URL : https://zakon.rada.gov.ua/laws/show/40-15#Text.

89. Про інформацію : Закон України від 2 жовт. 1992 р. Документ 2657-XII, чинний. Редакція від 20.01.2026. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

90. Про Кабінет Міністрів України: Закон України. Відомості Верховної

Ради (ВВР), 2014, № 13, ст.222. Документ 794-VII, чинний. Редакція від 13.12.2025. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text.

91. Про Концепцію оборони і будівництва Збройних Сил України : Постанова Верховної Ради України від 11.10.1991 № 1659-XII. URL: https://zakon.rada.gov.ua/laws/show/1659-12.

92. Про критичну інфраструктуру : Закон України від 16 лист. 2021 р. Документ 1882-IX, чинний. Редакція від 21.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

93. Про мобілізаційну підготовку та мобілізацію : Закон України від 21.10.1993 № 3543-XII. URL: https://zakon.rada.gov.ua/laws/show/3543-12.

94. Про національну безпеку України : Закон України від 21 черв. 2018 р. Документ 2469-VIII, чинний. Редакція від 24.01.2026. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

95. Про Національну гвардію України : Закон України від 13.03.2014 № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18.

96. Про оборонні закупівлі : Закон України від 17 верес. 2020 р. Документ 808-IX, чинний. Редакція від 28.08.2025. URL: https://zakon.rada.gov.ua/laws/show/808-20#Text.

97. Про оборону України : Закон України. Відомості Верховної Ради України (ВВР), 1992, № 9, ст.106. Документ 1932-XII, чинний. Редакція від 12.04.2026. https://zakon.rada.gov.ua/laws/show/1932-12#Text.

98. Про основи національного спротиву : Закон України. Відомості Верховної Ради (ВВР), 2021, № 41, ст.339. Документ 1702-IX, чинний. Редакція від 12.04.2026. https://zakon.rada.gov.ua/laws/show/1702-20#Text.

99. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15.

100. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. Документ 2163-VIII, чинний. Редакція від 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

101. Про правовий режим воєнного стану : Закон України від 12 трав. 2015

р. Документ 389-VIII, чинний. Редакція від 04.03.2026. URL: https://zakon.rada.gov.ua/laws/show/389-19.

102. Про проголошення незалежності України : Постанова Верховної Ради Української РСР від 24.08.1991 № 1427-XII. URL: https://zakon.rada.gov.ua/laws/show/1427-12.

103. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-вр.

104. Про Регламент Верховної Ради України : Закон України. Відомості Верховної Ради України (ВВР), 2010, № 14-15, № 16-17, ст.133. Документ 1861-VI, чинний. Редакція від 23.10.2026. https://zakon.rada.gov.ua/laws/show/1861-17#Text.

105. 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.

106. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

107. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 06.06.2016 № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/240/2016.

108. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 25 берез. 2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021.

109. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 25 берез. 2021 р. № 121/2021. URL:

https://zakon.rada.gov.ua/laws/show/121/2021.

110. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» : Указ Президента України від 14.03.2016 № 92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016.

111. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80.

112. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Документ 67-2018-р. Редакція від 17.09.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р.

113. Про часткову мобілізацію : Указ Президента України від 17.03.2014 № 303/2014. URL: https://zakon.rada.gov.ua/laws/show/303/2014.

114. Пустовіт Я. Б. Аналіз існуючих стратегій використання штучного інтелекту в обороні. *Національна безпека України в умовах воєнного стану* : І Науково-практична конференція з міжнародною участю, м. Чернігів, 6-8 березня 2024 року : тези доповіді / за заг. ред. З. В. Гбур. Чернігів : ІПТ, 2024. С. 212–216.

115. Пустовіт Я. Б. Аспект публічного управління: використання штучного інтелекту в обороноздатності України. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : І Міжнародна науково-практична конференція, 2 червня 2023 року : тези доповіді / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 224–226.

116. Пустовіт Я. Б. Використання штучного інтелекту в обороноздатності України. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : ІІ Міжнародна науково-практична конференція, 27 жовтня 2023 року : тези доповіді / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 192-195.

117. Пустовіт Я. Б. Державна політика використання штучного інтелекту в

оборонній сфері України. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : VII Міжнародна наукова конференція, м. Харків, 31 липня 2026 року : тези доповіді / Міжнародний центр наукових досліджень. Вінниця : ТОВ «УКРЛОГОС Груп», 2026. С. 56-58.

118. Пустовіт Я. Б. Державна політика щодо використання технологій штучного інтелекту у сфері оборони України. *Актуальні проблеми інноваційної економіки та права*. 2026. №3. С. 191-195. DOI: https://doi.org/10.36887/2524-0455-2026-3-36.

119. Пустовіт Я. Б. Нормативно-правова база використання штучного інтелекту в обороні. *Стратегічні пріоритети менеджменту і адміністрування у повоєнний період* : V Міжнародна науково-практична інтернет-конференція, 26 квітня 2024 року : тези доповіді. 2024. С. 150-153.

120. Пустовіт Я. Б. Обробка фінансової інформації в умовах війни: програми та технології. *Тренди сталого розвитку для України* : I Науково-практична конференція за міжнародною участю, м. Чернігів – м. Київ, 10 липня 2024 року : тези доповіді. Чернігів : УТМ, 2024. С. 80–84.

121. Пустовіт Я. Б. Теоретичні засади використання штучного інтелекту в системі публічного управління обороноздатністю держави. *Herald of Khmelnytskyi National University*. Economic Sciences. 2026. Вип. 356(4). С. 189-195. DOI: https://doi.org/10.31891/2307-5740-2026-356-26.

122. Пустовіт Я. Б. Цивільно-військове співробітництво в інноваційних розробках: політика щодо штучного інтелекту. *Сучасний стан та пріоритети модернізації науки, освіти, технологій та суспільства* : Міжнародна науково-практична конференція, м. Ізмаїл, 16 квітня 2025 року : тези доповіді. Ізмаїл : ЦФЕНД, 2025. С. 56-57.

123. Пустовіт Я. Б. Штучний інтелект та публічне управління. *Складові національної безпеки в умовах воєнного стан*у : Науково-практична конференція з міжнародною участю, м. Київ, 9-11 серпня 2023 року : тези доповіді / за заг. ред. З. В. Гбур. Кам’янець-Подільський : Друкарня Рута, 2023. С. 102–111.

124. Пустовіт Я. Б., Гбур З. В. Аналіз існуючих стратегій у державному

управлінні щодо використання штучного інтелекту в обороні. *Успіхи та досягнення в науці*. 2024. № 1(1). С. 172-185. DOI: https://doi.org/10.52058/3041-1254-2024-1(1)-172-185.

125. Пустовіт Я. Б., Гбур З. В. Використання штучного інтелекту в підвищенні обороноздатності України: аспекти публічного управління. *Інвестиції: практика та досвід*. 2023. № 13. С. 103-108. DOI: https://doi.org/10.32702/2306-6814.2023.13.103.

126. Пустовіт Я. Б., Палагусинець Р. В. Опис нормативно-правової бази використання штучного інтелекту в обороні, включаючи законодавство та міжнародні стандарти. Україна: проблеми і перспективи розвитку : колективна монографія / за заг. ред. З. В. Гбур. Чернігів : ППТ, 2024. С. 113–121.

127. Рада національної безпеки і оборони України. Офіційний вебсайт. URL: https://www.rnbo.gov.ua/.

128. Рамкова Конвенція Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права. URL : https://vkksu.gov.ua/sites/default/files/rye_ramkova_konvenciya_zi_shtuchnogo_intelektu_prav_lyudyny_demokratiyi_ta_verh._prava.pdf.

129. Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг та внесення змін до Директиви 2000/31/ЄС. URL : https://www.siemens.com/uk-ua/company/compliance/eu-digital-services-act/.

130. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту (Акт про штучний інтелект). Офіційний вісник Європейського Союзу. URL : https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

131. Регулювання штучного інтелекту в Україні: презентуємо Білу книгу. Міністерство цифрової трансформації України, 26 червня 2024 року. URL : https://thedigital.gov.ua/news/regulyuvannyashtuchnogo-intelektu-v-ukraini-prezentuemo-bilu-knigu.

132. Регулювання штучного інтелекту в Україні: презентуємо дорожню

карту. Міністерство цифрової трансформації України, 7 жовтня 2023. URL : https://thedigital.gov.ua/news/regulyuvannya-shtuchnogointelektu-v-ukraini-prezentuemo-dorozhnyu-kartu.

133. Регуляторні пісочниці у світі та в Україні: як експерименти змінюють ринок ШІ. Міністерство цифрової трансформації України. URL : https://thedigital.gov.ua/news/shtuchnyy-intelekt/rehuliatorni-pisochnytsi-u-sviti-ta-v-ukrayini-iak-eksperymenty-zminiuiut-rynok-shi.

134. Ризики, правові виклики та безпекові гарантії. *Вісник кримінологічної асоціації України*. 2025. №2 (35). Частина 2. С. 574-585. DOI: https://doi.org/10.32631/vca.2025.2.82.

135. Рудник Л. І. Правові засади обмеження права на доступ до інформації в умовах воєнного стану. *Вісник НТУУ «КПІ».* Політологія. Соціологія. Право. 2023. № 4 (60). С. 32–39. DOI: https://doi.org/10.20535/2308-5053.2023.4(60).296975.

136. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с. URL: https://readukrainianbooks.com/1314-svitova-gibridna-vijna-ukrayinskij-front-volodimir-pavlovich-gorbulin.htm.

137. Сироватко В. В. Обороноздатність та оборонна достатність як функціональний прояв оборонного потенціалу: уточнення понять. Регіональні студії. 2025. Вип. 41. С. 166–171. DOI: https://doi.org/10.32782/2663-6170/2025.41.27.

138. Споришев К. О. Аналіз нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки Україні. Честь і закон. 2024. №1 (88). С. 142–149.

139. Споришев К. О. Інформаційно-аналітичні технології сил безпеки у парадигмі державного управління. *Наукові інновації та передові технології* (Серія «Управління та адміністрування»). 2024. Вип. № 1(29). С. 128–136.

140. Споришев К. О. Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України: теорія,

методологія, практика : монографія. Одеса : Олді+, 2024. 312 с.

141. Стокгольмський міжнародний інститут досліджень миру. Незалежний ресурс з питань глобальної безпеки. URL : https://www.sipri.org/.

142. Стратегія розвитку штучного інтелекту в Україні на період до 2030 року. URL : https://storage.thedigital.gov.ua/files/7/b7/75857d83c873b507961901a10ef20b71.pdf

143. Територіальна цілісність України : Резолюція Генеральної Асамблеї ООН від 27.03.2014 № 68/262 (A/RES/68/262). URL: https://digitallibrary.un.org/record/767565.

144. Тєстоєдов О. А. Мотивація публічних службовців в період війни: роль розподіленого лідерства. *Публічне управління та митне адміністрування*. 2026. № 1 (48). С. 114-119. DOI : https://doi.org/10.32782/2310-9653-2026-1.17.

145. Торічний В. О., Максимів І. С. Управлінська мотивація у державній прикордонній службі: актуальні підходи і практики. *Безпека держави*. 2025. Том 1 № 5. URL : https://dspace.nadpsu.edu.ua/handle/123456789/5125.

146. У Збройних Силах України запущено єдину цифрову систему управління логістикою на базі SAP. URL : https://digitalbs.com.ua/novyny-ta-podiyi/u-zbrojnyh-sylah-ukrayiny-zapushheno-yedynu-czyfrovu-systemu-upravlinnya-logistykoyu-na-bazi-sap/.

147. У ЗСУ затвердили Концепцію використання ШІ та створили підрозділи для його тестування. 2026. URL : https://militarnyi.com/uk/news/u-zsu-zatverdyly-kontseptsiyu-shi/.

148. Україна приєдналася до Європейської ради зі штучного інтелекту. Прес-служба Кабінет Міністрів України, 31 жовтня 2025 року. URL : https://www.kmu.gov.ua/news/ukraina-pryiednalasia-do-ievropeiskoirady-zi-shtuchnoho-intelektu.

149. Українські AI-платформи. URL : https://catalog.ai.ua/platform/?sector=%D0%9E%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B0+%D1%82%D0%B0+%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.

150. Федоренко Т. В., Дабіжа В. В. Державне регулювання використання штучного інтелекту у сфері оборони україни: сучасний стан, виклики та напрями вдосконалення. *Український журнал прикладної економіки та техніки*. 2026. №3. С. 503-508. DOI: https://doi.org/10.36887/2415-8453-2026-3-90.

151. Харківський національний університет Повітряних Сил імені Івана Кожедуба. Офіційний сайт. URL : https://hups.mil.gov.ua/. ·

152. Чмир Я. І., Стілл А. В., Мошнін А. А., Рикунов Д. В. Механізми публічного управління: суть, роль та функції (на прикладі механізму контролю). *Публічне урядування*. 2024. № 3 (40), С. 50-57. DOI: https://doi.org/10.32689/2617-2224-2024-3(40)-7.

153. Шевченко А. І. та ін. Стратегія розвитку штучного інтелекту в Україні : монографія / за заг. ред. А. І. Шевченка. Київ : ІПШІ, 2023. 305 с. DOI: https://doi.org/10.15407/development_strategy_2023.

154. ШІ заощаджує до 90% часу на пошук ворожих цілей на фото й відео. Міністерство оборони України. 2026. URL : https://mod.gov.ua/news/shi-zaoshchadzhuie-do-90-chasu-na-poshuk-vorozhykh-tsilei-na-foto-y-video.

155. Шумлянський Д. В Україні створили центр розвитку оборонного ШІ. URL : https://militarnyi.com/uk/news/v-ukrayini-stvoryly-tsentr-oboronnogo-shi/.

156. Юхименко С. Регулювання штучного інтелекту: досвід ЄС та майбутнє регулювання в Україні. Аналітична записка. Інститут економічних досліджень та політичних консультацій, 2025. URL : http://www.ier.com.ua/files/Projects/2025/UA_EU/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%BE%D0%B3%D0%BE_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83.pdf.

157. Як Україна розробляє правила для штучного інтелекту. Пресслужба Апарату Верховної Ради України. 2026. URL : https://www.rada.gov.ua/news/news_kom/275189.html.

158. 23 липня 2014 року у Верховній Раді України відбулися парламентські

слухання на тему: «Обороноздатність України у XXI столітті: виклики, загрози та шляхи їх подолання». Верховна Рада України : офіційний вебпортал. 24.07.2014. URL: https://www.rada.gov.ua/print/96314.htm.

159. AI Act Service Desk. Recital 24. AI Act Single Information Platform. European Commission. URL: https://ai-act-service-desk.ec.europa.eu/en/ai-act/recital-24.

160. Artificial intelligence in the military domain and its implications for international peace and security : Resolution adopted by the General Assembly on 24 December 2024 : A/RES/79/239. New York : United Nations, 2024. URL: https://undocs.org/A/RES/79/239.

161. Australian Government. Defence Science and Technology Group. AI technology rises to the challenge. 10 January 2024. URL: https://www.dst.defence.gov.au/news/2024/01/10/ai-technology-rises-challenge.

162. Australian Government. Department of Defence. Defence Digital Strategy and Roadmap – 2025. Canberra, 2025. URL: https://www.defence.gov.au/sites/default/files/2025-11/Defence-Digital-Strategy-and-Roadmap-2025.pdf.

163. Australian Government. Department of Defence. Enhancing AI to support the warfighter. 9 August 2024. URL: https://www.defence.gov.au/news-events/news/2024-08-09/enhancing-ai-support-warfighter.

164. Australian Government. Department of Defence. Policy Settings for Responsible Use of Artificial Intelligence in Defence. 2026. URL: https://www.defence.gov.au/sites/default/files/2026-03/Policy-Settings-for-Responsible-Use-of-Artificial-Intelligence-in-Defence-%5BOFFICIAL%5D.pdf.

165. AI-екосистема України: таланти, компанії, освіта. AI HOUSE. 2024. URL : https://aihouse.org.ua/wp-content/uploads/2024/01/AI-Ecosystem-of-Ukraine-by-AI-HOUSE-x-Roosh-UA.pdf.

166. Boole G. An Investigation of the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities. London : Walton and Maberly. 1854. 424 p. DOI: https://doi.org/10.5962/bhl.title.29413.

167. Boulanin V., Davison N., Goussac N., Peldán Carlsson M. Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control. Stockholm : SIPRI ; Geneva : ICRC, 2020. URL: https://www.sipri.org/publications/2020/other-publications/limits-autonomy-weapon-systems-identifying-practical-elements-human-control-0.

168. Boulanin V., Palayer J., Ovink C. Addressing the Risks that Civilian AI Poses to International Peace and Security: The Role of Responsible Innovation. Stockholm : SIPRI, 2025. DOI: https://doi.org/10.55163/OXHH2798.

169. Boulanin V., Verbruggen M. Mapping the Development of Autonomy in Weapon Systems. Stockholm : SIPRI, 2017. URL: https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems.

170. Brave1 : платформа оборонних технологій України. URL: https://brave1.gov.ua.

171. Bullock J. B. Artificial Intelligence, Discretion, and Bureaucracy. The American Review of Public Administration. 2019. Vol. 49, No. 7. P. 751–761. DOI: https://doi.org/10.1177/0275074019856123.

172. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling online disinformation: a European Approach. URL: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018DC023.

173. Dartmouth College. The Research Conference Where AI Began. URL: https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth.

174. Dave P., Dastin J. Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition During War. Reuters. 2022. 13 March. URL: https://tech.yahoo.com/general/articles/exclusive-ukraine-started-using-clearview-200230843.html.

175. Defense AI Center «A1»: Міноборони прискорює впровадження штучного інтелекту у війну. Міністерство оборони України. 2026. URL: https://mod.gov.ua/news/defense-ai-center-a1-minoboroni-priskoryuye-

vprovadzhennya-shtuchnogo-intelektu-u-vijnu.

176. Defense AI Center A1. URL: https://catalog.ai.ua/tool/defense-ai-center-a1/.

177. Delipetrev B., Tsinaraki C., Kostić U. AI Watch: Historical Evolution of Artificial Intelligence. Analysis of the Three Main Paradigm Shifts in AI. Luxembourg : Publications Office of the European Union, 2020. 31 p. (EUR 30221 EN; JRC120469). ISBN 978-92-76-18940-4. DOI: https://doi.org/10.2760/801580.

178. Dolinko I., Antebi L. Embracing the Organized Mess: Defense AI in Israel. The Very Long Game / ed. by H. Borchert, T. Schütz, J. Verbovszky. Cham : Springer, 2024. P. 397–420. DOI: https://doi.org/10.1007/978-3-031-58649-1_18.

179. Drucker Peter F. The Practice of Management. Publisher : Oxford : Butterworth-Heinemann, 1999. 399 p.

180. Dwivedi Y. K., Sharma A., Rana N. P., Giannakis M., Goel P., Dutot V. Evolution of artificial intelligence research in Technological Forecasting and Social Change: Research topics, trends, and future directions. Technological Forecasting and Social Change. 2023. Vol. 192. Art. 122579. 17 p. DOI: https://doi.org/10.1016/j.techfore.2023.122579.

181. Ethics guidelines for trustworthy AI. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

182. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/

183. Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. 2023. URL: https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document05_en.pdf.

184. International Committee of the Red Cross. Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision-Making. Geneva : ICRC, 2024. URL: https://www.icrc.org/en/publication/decisions-decisions-decisions-computation-and-artificial-intelligence-military-decision.

185. ISO/IEC 42001:2023. Information technology - Artificial intelligence - Management system. Geneva : ISO, IEC, 2023. 51 p. URL: https://www.iso.org/standard/42001.

186. Israel Ministry of Defense. Israel MOD Establishes AI and Autonomy Administration. 2025. URL: https://mod.gov.il/en/press-releases/press-room/israel-mod-establishes-ai-and-autonomy-administration.

187. Israel Ministry of Defense. This is the First Robotics War – Tens of Thousands of Autonomous Systems Deployed Across All Domains. 2025. URL: https://mod.gov.il/en/press-releases/press-room/this-is-the-first-robotics-war-tens-of-thousands-of-autonomous-systems-deployed-across-all-domains.

188. Japan Ministry of Defense. Guidelines on Responsible Application of AI in the Research and Development of Defense Equipment. 6 June 2025. URL: https://www.mod.go.jp/atla/soubiseisaku/ai_guideline/ai_guideline_ver.01_eng_202506.pdf.

189. Japan Ministry of Defense. Ministry of Defense Basic Policy on Promoting the Utilization of AI. 2 July 2024. URL: https://www.mod.go.jp/en/article/2024/07/92d48f0d92e0e17facfe2235a5c00a77a0a3aed3.html.

190. Law Library of Congress. Use of Artificial Intelligence During Times of Conflict. Washington, D.C. : Library of Congress, 2025. URL: https://tile.loc.gov/storage-services/service/ll/llglrd/2025291260/2025291260.pdf.

191. Losing Humanity The Case against Killer Robots. New York : Human Rights Watch, 2012. 50 p.. URL: https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots.

192. McCarthy J., Hayes P. J. Some Philosophical Problems from the Standpoint of Artificial Intelligence. Machine Intelligence. 1969. Vol. 4. P. 463–502.

193. McCarthy J., Minsky M. L., Rochester N., Shannon C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence: August 31, 1955. AI Magazine. 2006. Vol. 27, № 4. P. 12–14. DOI: https://doi.org/10.1609/aimag.v27i4.1904.

194. Mearsheimer J. J. The Case for a Ukrainian Nuclear Deterrent. Foreign Affairs. 1993. Vol. 72, No. 3. P. 50–66.

195. Ministère des Armées. AMIAD, une agence clé pour l'IA de défense. 1 août

2025. URL: https://www.defense.gouv.fr/amiad-agence-ia-defense.

196. Ministère des Armées. IA de défense : quels enjeux pour les armées françaises ? 10 février 2025. URL: https://www.defense.gouv.fr/actualites/ia-defense-quels-enjeux-armees-francaises.

197. Ministère des Armées. IA de défense : Sébastien Lecornu inaugure le pôle recherche de l'Amiad. 5 mars 2025. URL: https://www.defense.gouv.fr/actualites/ia-defense-sebastien-lecornu-inaugure-pole-recherche-lamiad.

198. Ministère des Armées. Sébastien Lecornu lance la stratégie ministérielle sur l'intelligence artificielle. 8 mars 2024. URL: https://www.defense.gouv.fr/actualites/sebastien-lecornu-lance-strategie-ministerielle-lintelligence-artificielle.

199. Minsky M. Steps Toward Artificial Intelligence. Proceedings of the IRE. 1961. Vol. 49, No. 1. P. 8–30. DOI: https://doi.org/10.1109/JRPROC.1961.287775.

200. NATO. Alliance Digital Strategy. 13 January 2026. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/01/13/alliance-digital-strategy.

201. NATO. NATO releases revised AI strategy. NATO : News. 10 July 2024. URL: https://www.nato.int/en/news-and-events/articles/news/2024/07/10/nato-releases-revised-ai-strategy.

202. NATO. Summary of NATO's revised Artificial Intelligence (AI) strategy. NATO : Official texts. 10 July 2024. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

203. NIST. Artificial Intelligence Risk Management Framework. URL: https://www.nist.gov/itl/ai-risk-management-framework.

204. Norton W. W. & Company. Scharre P. Army of None: Autonomous Weapons and the Future of War. URL: https://ftp.idu.ac.id/wp-content/uploads/ebook/tdg/MILITARY%20PLATFORM%20DESIGN/Army%20of%20None%20Autonomous%20Weapons%20and%20the%20Future%20of%20War.pdf.

205. OECD. Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions. Paris : OECD Publishing, 2025. 306 p. DOI: https://doi.org/10.1787/795de142-en.

206. PerryJ.L., Wise L.R.TheMotivational BasesofPublicService. Public Administration Review. 1990. Vol. 50, No. 3. P. 367-373.

207. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy / U.S. Department of State. Washington, 2023. URL: https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy.

208. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng.

209. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.

210. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

211. Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems of the High Contracting Parties to the Convention on Certain Conventional Weapons : CCW/GGE.1/2019/3. Geneva : United Nations, 2019. URL: https://undocs.org/CCW/GGE.1/2019/3.

212. Reznik N., Lazebnyk V., Pitel N., Klymenko L., Kustrich L., Vuichenko M., Zahorodnia A. Logistical Management as an Instrument of Optimization of Flowing Processes of Contemporary Organizations in the Context of European Integration. Big Data in Finance: Transforming the Financial Landscape / ed. by B.

Alareeni. Cham : Springer, 2025. Vol. 164 (Studies in Big Data). P. 355–367. DOI: https://doi.org/10.1007/978-3-031-75095-3_29.

213. Russell S. J., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Hoboken : Pearson, 2021. 1136 p.

214. Söğüt H. E., Usta S. Artificial Intelligence in Public Administration: A Comprehensive Bibliometric Review. International Journal of Contemporary Economics and Administrative Sciences. 2026. URL: https://www.ijceas.com/ijceas/article/view/1062.

215. Sporyshev K. Theoretical basis of the information and analytical support development of the security forces of Ukraine: aspects of state governance. International security studios: managerial, technical, legal, environmental, informative and psychological aspects. International collective monograph. Vol. I. Oslo, Kingdom of Norway, 2024. Pp. 379-407.

216. Stanford University. One Hundred Year Study on Artificial Intelligence. Appendix I: A Short History of AI. 2016. URL: https://ai100.stanford.edu/reports/2016-report/appendix-i-short-history-ai.

217. Summary of NATO's revised Artificial Intelligence (AI) strategy / NATO. Brussels, 10 July 2024. URL: https://www.nato.int/cps/en/natohq/official_texts_227237.htm.

218. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD : National Institute of Standards and Technology, 2023. NIST AI 100-1. DOI: https://doi.org/10.6028/NIST.AI.100-1.

219. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

220. Turing A. M. Computing Machinery and Intelligence. Mind. 1950. Vol. 59, Issue 236. P. 433–460. DOI: https://doi.org/10.1093/mind/LIX.236.433.

221. UK Ministry of Defence. Defence Artificial Intelligence Strategy. London, 2022. 72 p. URL:

https://assets.publishing.service.gov.uk/media/62a7543ee90e070396c9f7d2/Defence_Artificial_Intelligence_Strategy.pdf.

222. UK Ministry of Defence. Putting Artificial Intelligence (AI) at the Heart of UK Defence. 10 June 2026. URL: https://www.gov.uk/government/publications/putting-artificial-intelligence-ai-at-the-heart-of-uk-defence/putting-artificial-intelligence-ai-at-the-heart-of-uk-defence.

223. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021. URL: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics.

224. Vandenabeele W., Ritz A., Neumann O. Public service motivation: state of the art and conceptual cleanup. The Palgrave Handbook of Public Administration and Management in Europe / Ed. by E. Ongaro, S. van Thiel. London: Palgrave Macmillan, 2018. P. 261–278.

225. Von der Leyen U. A Union that strives for more. My agenda for Europe: Political Guidelines for the Next European Commission 2019–2024. Luxembourg : Publications Office of the European Union, 2019. 24 p. URL: https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf.

226. White Paper on Artificial Intelligence: A European approach to excellence and trust. European Commision. Brussels, 19.2.2020. COM(2020) 65 final. URL: https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065.

227. Wirtz B. W., Weyerer J. C., Geyer C. Artificial Intelligence and the Public Sector—Applications and Challenges. International Journal of Public Administration. 2019. Vol. 42, No. 7. P. 596–615. DOI: https://doi.org/10.1080/01900692.2018.1498103.

228. Yarovoi T. Analysis of the models of protection of the state security. Legea si Viata (Republic Moldova). 2019. № 8. С. 144–148.

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

1. **Пустовіт Я. Б.,** Гбур З. В. Використання штучного інтелекту в підвищенні обороноздатності України: аспекти публічного управління. *Інвестиції: практика та досвід.* 2023. № 13. С. 103-108. DOI: https://doi.org/10.32702/2306-6814.2023.13.103. *(Пустовіт Я. Б. – досліджено можливості використання технологій штучного інтелекту для підвищення обороноздатності України, визначено перспективні напрями їх застосування в секторі безпеки і оборони. Гбур З. В. – розглянуто особливості публічного управління процесами впровадження технологій штучного інтелекту та організаційно-управлінські аспекти їх використання для забезпечення обороноздатності держави).*

2. **Пустовіт Я. Б.,** Гбур З. В. Аналіз існуючих стратегій у державному управлінні щодо використання штучного інтелекту в обороні. *Успіхи та досягнення в науці.* 2024. № 1(1). С. 172-185. DOI: https://doi.org/10.52058/3041-1254-2024-1(1)-172-185. *(Пустовіт Я.Б. – проаналізовано наявні стратегії використання штучного інтелекту в оборонній сфері, визначено основні напрями його застосування для підвищення ефективності оборонної діяльності та підтримки прийняття стратегічних рішень. Гбур З. В. досліджено організаційно-управлінські, нормативно-правові та етичні аспекти впровадження штучного інтелекту в оборонній сфері).*

3. Пустовіт Я. Б. Державна політика щодо використання технологій штучного інтелекту у сфері оборони України. *Актуальні проблеми інноваційної економіки та права.* 2026. №3. С. 191-195. DOI: https://doi.org/10.36887/2524-0455-2026-3-36.

4. Пустовіт Я. Б. Теоретичні засади використання штучного інтелекту в

системі публічного управління обороноздатністю держави. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. Вип. 356(4). С. 189-195. DOI: https://doi.org/10.31891/2307-5740-2026-356-26.

Тези наукових доповідей

5. Пустовіт Я. Б. Обробка фінансової інформації в умовах війни: програми та технології. *Тренди сталого розвитку для України* : І Науково-практична конференція за міжнародною участю, м. Чернігів – м. Київ, 10 липня 2024 року : тези доповіді. Чернігів : УТМ, 2024. С. 80-84.

6. Пустовіт Я. Б. Аспект публічного управління: використання штучного інтелекту в обороноздатності України. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : І Міжнародна науково-практична конференція, м. Переяслав, 2 червня 2023 року : тези доповіді / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 224-226.

7. Пустовіт Я. Б. Штучний інтелект та публічне управління. *Складові національної безпеки в умовах воєнного стану* : Науково-практична конференція з міжнародною участю, м. Київ, 9-11 серпня 2023 року : тези доповіді / за заг. ред. З. В. Гбур. Кам'янець-Подільський : Друкарня Рута, 2023. С. 102-111.

8. Пустовіт Я. Б. Використання штучного інтелекту в обороноздатності України. *Сучасні аспекти реформування системи публічного управління в умовах воєнного часу* : ІІ Міжнародна науково-практична конференція, м. Переяслав, 27 жовтня 2023 року : тези доповіді / за заг. ред. О. І. Пархоменко-Куцевіл. Переяслав, 2023. С. 192-195.

9. Пустовіт Я. Б. Нормативно-правова база використання штучного інтелекту в обороні. *Стратегічні пріоритети менеджменту і адміністрування у повоєнний період* : V Міжнародна науково-практична інтернет-конференція, м. Харків, 26 квітня 2024 року : тези доповіді. 2024. С. 150-153.

10. Пустовіт Я. Б. Аналіз існуючих стратегій використання штучного інтелекту в обороні. *Національна безпека України в умовах воєнного стану* : І Науково-практична конференція з міжнародною участю, м. Чернігів, 6-8 березня 2024 року : тези доповіді / за заг. ред. З. В. Гбур. Чернігів : ІПТ, 2024. С. 212-216.

11. Пустовіт Я. Б. Цивільно-військове співробітництво в інноваційних розробках: політика щодо штучного інтелекту. *Сучасний стан та пріоритети модернізації науки, освіти, технологій та суспільства* : Міжнародна науково-практична конференція, м. Ізмаїл, 16 квітня 2025 року : тези доповіді. Ізмаїл : ЦФЕНД, 2025. С. 56-57.

12. Пустовіт Я. Б. Державна політика використання штучного інтелекту в оборонній сфері України. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : VII Міжнародна наукова конференція, м. Харків, 31 липня 2026 року : тези доповіді / Міжнародний центр наукових досліджень. Вінниця : ТОВ «УКРЛОГОС Груп», 2026. С. 56–58.

Довідки про впровадження

Додаток Б

Заклад вищої освіти
"Відкритий
міжнародний УНІВЕРСИТЕТ
розвитку людини
"УКРАЇНА"

Higher Education Institution
"Open
International UNIVERSITY
of Human Development
"UKRAINE"

Україна, 03115, м. Київ, вул. Львівська, 23, тел.: 044-409-27-69, 067-406-53-92, 067-328-28-22
e-mail: office@uu.edu.ua; viddilorgrobotu@ukr.net сайт: http://uu.edu.ua

№ 123-273 від 05. лютого 2026 р.

ДОВІДКА

Видана здобувачу освіти **Пустовіту Ярославу Борисовичу** про те, що він у ході виконання дисертаційного дослідження на тему **«Використання штучного інтелекту в підвищенні обороноздатності України: аспект публічного управління»** приймав участь у виконанні науково-дослідної теми кафедри міжнародних відносин та політичного консалтингу «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (№ державної реєстрації 0124U000322).

Директор Інституту права та суспільних відносин **Тетяна ФЕДОРЕНКО**

Додаток В

Заклад вищої освіти
"Відкритий
міжнародний УНІВЕРСИТЕТ
розвитку людини
"УКРАЇНА"

Higher Education Institution
"Open
International UNIVERSITY
of Human Development
"UKRAINE"

Україна, 03115, м. Київ, вул. Львівська, 23, тел.: 044-409-27-69, 067-406-53-92, 067-328-28-22
e-mail: office@uu.edu.ua; viddilorgrobotu@ukr.net сайт: http://uu.edu.ua

№ 13/2 3-272 від 05 лютого 2026 р.

Довідка

про впровадження

результатів наукового дослідження у навчальний процес

видана **Пустовіту Ярославу Борисовичу** про те, що результати його дисертаційного дослідження на здобуття наукового ступеня доктора філософії на тему **«Використання штучного інтелекту в підвищенні обороноздатності України: аспект публічного управління»** за спеціальністю 281 «Публічне управління та адміністрування» були використані при розробці робочих програм, силабусів, а також під час викладання таких навчальних дисциплін як «Інформаційні війни» за програмою підготовки фахівців освітнього рівня «магістр», «Міжнародна та національна безпека» за програмою підготовки фахівців освітнього рівня «магістр».

Завідувач кафедри міжнародних відносин
та політичного консалтингу
Інституту права та суспільних відносин
ЗВО «Відкритий міжнародний університет
розвитку людини «Україна»
к.пол.н., доцент **Тетяна КАДЛУБОВИЧ**

Додаток Г

Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів
вул. Бориса Грінченка, 1, 2-й поверх, м. Київ, 01001
№ 02-35/2026 від 21.09. 2026 р.

ДОВІДКА

про впровадження результатів дисертаційного дослідження **Пустовіта Ярослава Борисовича** на тему **«Використання штучного інтелекту в підвищенні обороноздатності України: аспект публічного управління»** на здобуття наукового ступеня докора філософії в галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування»

видано Пустовіту Я. Б., здобувачу ступеня доктора філософії, про те, що положення та результати його дисертаційного дослідження на тему «Використання штучного інтелекту в підвищенні обороноздатності України: аспект публічного управління», виконаного на кафедрі міжнародних відносин та політичного консалтингу у ЗВО «Відкритий міжнародний університет розвитку людини «Україна», становлять практичний інтерес для діяльності Управління виявлення та розшуку активів Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, у частині вдосконалення інформаційно-аналітичного забезпечення, розвитку цифрових інструментів аналізу даних та підвищення ефективності прийняття управлінських рішень.

Зокрема, практичне значення мають наукові положення щодо систематизації функціональних можливостей штучного інтелекту в публічному управлінні, використання інтелектуальних технологій для автоматизованого опрацювання значних масивів інформації, виявлення взаємозв'язків між даними з різних інформаційних джерел, а також інформаційно-аналітичної підтримки прийняття управлінських рішень.

Окремий практичний інтерес становлять обґрунтовані в дисертаційному дослідженні підходи до вдосконалення організаційних та інституційних механізмів упровадження технологій штучного інтелекту, які можуть бути адаптовані до процесів аналізу інформації про активи, встановлення зв'язків між суб'єктами та об'єктами майнових відносин, систематизації відомостей із державних реєстрів та інших інформаційних ресурсів з дотриманням вимог законодавства.

Науково-практичні положення та рекомендації у дисертаційному дослідженні використано під час підготовки матеріалів, що стосуються перспектив застосування інтелектуальних технологій у процесах інформаційно-аналітичного забезпечення діяльності з виявлення та розшуку

активів, удосконалення підходів до оброблення й систематизації інформації та підтримки прийняття управлінських рішень.

Практичне значення результатів дисертаційного дослідження полягає у можливості їх використання для розвитку інформаційно-аналітичних інструментів, удосконалення управлінських процесів та підвищення ефективності діяльності у сфері виявлення та розшуку активів шляхом застосування сучасних технологій штучного інтелекту.

Начальник Управління виявлення та розшуку активів Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів **Ніна МИРОНЮК**

Начальник
Управління персоналу