analyzes the functioning of video surveillance systems and their role in maintaining public order, road safety, and combating criminal offenses. The main directions for the development of "Safe City" projects and prospects for their integration into a unified national digital security system are identified. The research showed that implementing "Safe City" programs is an important direction for increasing the effectiveness of state policy in ensuring public safety. The use of modern video surveillance systems, automated information analysis tools, and integrated mechanisms for interaction between various services contributes to increasing the effectiveness of preventing offenses and responding to emergencies. In general, "Safe City" is a city video surveillance system designed to record violations and automatically respond to them. Promising areas of further research include improving mechanisms for integrating artificial intelligence systems into Safe City projects, developing unified standards for the functioning of security systems, and researching issues of information and personal data protection.

Keywords: *state regulation; information security; public administration; state policy; digital threats; cyber threats; hybrid threats; information risks; information infrastructure; national security, social policy of the city, social development of the city.*

Стаття надійшла до редакції / Received 24.05.2026 Прийнята до друку / Accepted 20.06.2026 Опубліковано/ Published 08.08.2026

Бібліографічний опис статті:

Пустовіт О.Б. Передумови та цілі впровадження проєктів «Безпечне місто» на державному рівні. Актуальні проблеми інноваційної економіки та права. 2026. № 3. С. 187-191.

Pustovit O. Prerequisites and goals for implementing "Safe City" projects at the state level. Actual problems of innovative economy and law. 2026. No. 3, pp. 187-191.

УДК: 351:355.4:004.8; JEL classification: H11, H56, O38, O33 DOI: https://doi.org/10.36887/2524-0455-2026-3-36

ПУСТОВІТ Ярослав Борисович, аспірант кафедри управління охороною здоров'я та публічного адміністрування Національного університету охорони здоров'я України імені П.Л. Шупика, м. Київ, Україна, https://orcid.org/0009-0006-4572-1743

ДЕРЖАВНА ПОЛІТИКА ЩОДО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ОБОРОНИ УКРАЇНИ

Пустовіт Я.Б. Державна політика щодо використання технологій штучного інтелекту у сфері оборони України.

У статті досліджено особливості формування державної політики щодо використання технологій штучного інтелекту як одного з ключових чинників підвищення обороноздатності України в умовах сучасних безпекових викликів. Обґрунтовано, що цифрова трансформація сектору безпеки й оборони зумовлює необхідність переосмислення підходів до публічного управління, орієнтованого на впровадження інноваційних технологій, підвищення ефективності управлінських рішень і забезпечення технологічної переваги держави. Розкрито сутність державної політики у сфері використання штучного інтелекту в обороні, визначено його основні функції як інструменту інформаційно-аналітичного забезпечення, підтримки прийняття управлінських рішень, розвитку кібероборони, автономних систем, оборонної логістики та інформаційної безпеки. Проаналізовано сучасні підходи до розуміння обороноздатності держави та встановлено, що її забезпечення дедалі більше залежить від рівня цифровізації, розвитку інформаційних технологій, кіберстійкості та ефективності державного управління. Особливу увагу приділено визначенню ключових функцій держави у сфері публічного управління використанням технологій штучного інтелекту, серед яких стратегічна, нормативно-правова, інституційна, ресурсна, кадрова та контрольна. Доведено, що їх комплексна реалізація створює необхідні передумови для ефективної інтеграції технологій штучного інтелекту в сектор безпеки й оборони, забезпечує розвиток оборонних інновацій, зміцнення національної безпеки та підвищення обороноздатності України.

Ключові слова: *штучний інтелект, публічне управління, державна політика, обороноздатність, сектор безпеки і оборони, цифрова трансформація, національна безпека, кібербезпека, оборонні технології.*

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© ПУСТОВІТ Ярослав Борисович, 2026

Постановка проблеми у загальному вигляді. В умовах повномасштабної збройної агресії проти України, стрімкого розвитку цифрових технологій та трансформації сучасного безпекового середовища одним із ключових пріоритетів державної політики стає підвищення обороноздатності держави шляхом впровадження інноваційних технологій. Особливого значення в цьому процесі набуває використання штучного інтелекту, який сьогодні розглядається не лише як перспективний інструмент автоматизації окремих процесів, а й як стратегічний ресурс, здатний суттєво підвищити ефективність функціонування сектору безпеки й оборони. Технології штучного інтелекту забезпечують нові можливості для аналізу великих масивів даних, підтримки прийняття управлінських рішень, розвитку безпілотних та автономних систем, кібероборони, оборонної логістики, прогнозування загроз і протидії інформаційним операціям.

Водночас ефективність застосування технологій штучного інтелекту визначається не лише рівнем їх технологічного розвитку, а й якістю державного управління, наявністю комплексної державної політики, сучасного нормативно-правового забезпечення, достатнього ресурсного потенціалу, ефективної міжвідомчої взаємодії та системи державного контролю. Саме тому питання використання штучного інтелекту виходить за межі виключно технічної проблематики та набуває характеру комплексного публічно-управлінського завдання, що потребує наукового осмислення механізмів формування й реалізації відповідної державної політики.

Актуальність дослідження зумовлена також необхідністю адаптації системи публічного управління України до сучасних безпекових викликів, інтеграції міжнародного досвіду використання технологій штучного інтелекту в оборонній сфері, розвитку цифрової трансформації сектору безпеки й оборони, а також забезпечення технологічної переваги держави в умовах ведення сучасної війни. Розв'язання зазначених проблем безпосередньо пов'язане з виконанням стратегічних завдань державної політики у сфері національної безпеки, зміцненням обороноздатності України, підвищенням ефективності діяльності органів публічної влади та реалізацією курсу на цифровізацію державного управління.

Отже, дослідження державної політики щодо використання технологій штучного інтелекту для підвищення обороноздатності України є важливим як з наукового, так і з практичного погляду, оскільки його результати можуть стати основою для вдосконалення механізмів публічного управління, нормативно-правового регулювання та організаційного забезпечення цифрової трансформації сектору безпеки й оборони.

Аналіз останніх досліджень і публікацій. Проблематика використання технологій штучного інтелекту в публічному управлінні та секторі безпеки й оборони останніми роками набула особливої актуальності. Наукові дослідження охоплюють питання державного регулювання, цифрової трансформації, управління ризиками, кібербезпеки, розвитку автономних систем та впровадження штучного інтелекту у процеси прийняття управлінських рішень.

Серед зарубіжних дослідників вагомий внесок у розвиток концепції державного управління технологіями штучного інтелекту зробили С.А. Баркат та М. Бусідос, які дослідили особливості використання алгоритмічних систем у діяльності органів публічної влади та вплив автоматизованих рішень на державне управління.

Проблемам застосування штучного інтелекту в оборонній сфері присвячені праці М. Драсара, А. Котта, П. Лебланка, П. Терона, та інших учених, які в межах

дослідницьких програм НАТО розробили концепцію автономних інтелектуальних агентів кібероборони (AICA), визначивши архітектуру та перспективи використання штучного інтелекту для захисту військових інформаційних систем.

Окремий напрям досліджень становлять питання державної політики та міжнародного регулювання використання штучного інтелекту. Значний внесок у розвиток концепції відповідального управління штучним інтелектом зробила В. Хардінг, яка обґрунтовує необхідність поєднання технологічних інновацій із демократичним врядуванням, прозорістю та підзвітністю державних інституцій.

Серед вітчизняних науковців можна виокремити праці З. Ґбур, В. Савченко, О. Шаповаленко, С. Шумлянського, Є. Хоменко.

Водночас, незважаючи на значний науковий доробок у сфері цифрових технологій, кібербезпеки та оборонних інновацій, недостатньо дослідженими залишаються саме публічно-управлінські механізми використання штучного інтелекту для підвищення обороноздатності України. Потребують подальшого наукового обґрунтування питання формування комплексної державної політики, визначення функцій органів публічної влади, інституційного забезпечення, міжвідомчої координації, кадрової політики, ресурсного забезпечення та державного контролю за впровадженням технологій штучного інтелекту в секторі безпеки й оборони.

Формулювання цілей статті (постановка завдання). Незважаючи на активний розвиток наукових досліджень у сфері цифрової трансформації державного управління, національної безпеки та застосування технологій штучного інтелекту, недостатньо дослідженими залишаються питання формування комплексної державної політики щодо використання штучного інтелекту саме у сфері оборони України. Наявні наукові праці переважно зосереджені на технічних аспектах функціонування систем штучного інтелекту, кібербезпеці, автономному озброєнні або правовому регулюванні окремих цифрових технологій. Водночас потребують подальшого наукового обґрунтування організаційно-управлінські механізми впровадження штучного інтелекту в секторі безпеки й оборони, визначення функцій держави в цьому процесі, а також особливості міжвідомчої координації, ресурсного забезпечення, кадрової підготовки та системи державного контролю. Крім того, недостатньо розробленими залишаються теоретико-методологічні підходи до інтеграції технологій штучного інтелекту в систему публічного управління як інструменту підвищення обороноздатності держави в умовах сучасних воєнних і гібридних загроз. Саме необхідність комплексного дослідження зазначених аспектів зумовила вибір теми статті та визначила її наукову спрямованість.

Метою статті є дослідження теоретико-методологічних засад формування державної політики щодо використання технологій штучного інтелекту у сфері оборони України, визначення його ролі у підвищенні обороноздатності держави, а також обґрунтування основних функцій публічного управління, необхідних для ефективного впровадження та використання технологій штучного інтелекту в секторі безпеки й оборони.

Виклад основного матеріалу дослідження. Державна політика у сфері оборони є одним із ключових напрямів діяльності держави, спрямованим на забезпечення суверенітету, територіальної цілісності, воєнної безпеки, захисту населення та національних інтересів. У сучасних умовах її зміст істотно трансформується під впливом цифровізації, розвитку високотехнологічного озброєння, інформаційного протиборства, кіберзагроз, автономних систем і технологій штучного інтелекту.

У широкому розумінні державну політику щодо використання технологій штучного інтелекту у сфері оборони доцільно розглядати як систему цілей, принципів, рішень, інструментів і дій органів публічної влади, спрямованих на забезпечення ефективного, безпечного, відповідального та стратегічно орієнтованого впровадження технологій штучного інтелекту в сектор безпеки й оборони [9].

Така політика має міжгалузевий характер, оскільки перебуває на перетині публічного управління, національної безпеки, оборонного планування, цифрової трансформації, інформаційної політики, правового регулювання, інноваційної політики та міжнародного співробітництва. Її специфіка полягає в тому, що об'єктом управлінського впливу виступають не лише технології як такі, а й увесь комплекс суспільних, організаційних, правових і безпекових відносин, що виникають у процесі їх розроблення, впровадження та використання.

З позицій публічного управління штучний інтелект у сфері оборони виконує кілька ключових функцій.

По-перше, він є інструментом інформаційно-аналітичного забезпечення управлінських рішень. Алгоритми штучного інтелекту здатні обробляти великі масиви даних, виявляти закономірності, прогнозувати розвиток ситуації, здійснювати класифікацію ризиків і підтримувати прийняття рішень в умовах невизначеності [1].

По-друге, штучний інтелект є засобом підвищення оперативності управління. У сфері оборони час прийняття рішення часто має критичне значення. Автоматизована обробка даних дозволяє скоротити часові витрати на аналіз інформації, підвищити швидкість реагування на загрози та забезпечити точніше планування дій [2].

По-третє, штучний інтелект є чинником технологічної переваги. Його застосування у безпілотних системах, розвідувальних комплексах, кібероборoні, логістиці та системах управління може забезпечити якісну перевагу над противником навіть за умов обмеженості матеріальних ресурсів [3].

По-четверте, штучний інтелект є предметом державного регулювання та контролю. Оскільки його використання у сфері оборони пов'язане з ризиками помилкових рішень, несанкціонованого доступу, алгоритмічної упередженості, втрати контролю над автономними системами та порушення норм міжнародного права, держава має забезпечити належні механізми правового, етичного й організаційного контролю [4].

Отже, державна політика щодо використання штучного інтелекту у сфері оборони має бути спрямована не лише на стимулювання інновацій, а й на створення безпечної, контрольованої, відповідальної та ефективної системи його застосування.

Обороноздатність держави є комплексною характеристикою, що відображає її спроможність захищати суверенітет, територіальну цілісність і національні інтереси від зовнішніх і внутрішніх загроз. У сучасних умовах вона залежить не лише від класичних військових ресурсів, а й від рівня технологічного розвитку, ефективності управління, інформаційної стійкості, кіберзахищеності, інноваційного потенціалу та здатності держави швидко адаптуватися до нових форм ведення війни.

Обороноздатність держави є однією з фундаментальних категорій у сфері національної безпеки та публічного управління, оскільки визначає спроможність держави забезпечувати власний суверенітет, територіальну цілісність і незалежність в умовах зовнішніх і внутрішніх загроз [5].

В умовах трансформації сучасного безпекового середовища, розвитку гібридних загроз, кібероперацій, інформаційних атак та широкого використання новітніх цифрових технологій традиційне розуміння обороноздатності суттєво розширюється, охоплюючи не лише військовий компонент, а й економічний, технологічний, інформаційний, соціальний та управлінський потенціал держави.

Відповідно до Закону України «Про оборону України», обороноздатність держави визначається як здатність держави до захисту у разі збройної агресії або збройного конфлікту. Законодавець підкреслює, що

обороноздатність формується із сукупності матеріальних і духовних елементів та включає воєнний, економічний, соціальний і морально-політичний потенціал держави у сфері оборони, а також належні умови для його ефективної реалізації [8]. Таке визначення свідчить про комплексний характер обороноздатності, яка залежить не лише від рівня розвитку Збройних Сил України, а й від ефективності функціонування системи державного управління, економічної стійкості, розвитку науки й технологій, рівня суспільної консолідації та готовності населення до захисту держави [12].

Матеріальна складова обороноздатності охоплює військовий потенціал держави, сучасне озброєння та військову техніку, оборонно-промисловий комплекс, логістичне забезпечення, фінансові ресурси, критичну інфраструктуру та технологічні можливості країни. Саме ці компоненти забезпечують практичну спроможність держави вести оборонні дії, швидко реагувати на військові загрози та підтримувати стійке функціонування сектору безпеки і оборони в умовах війни.

Не менш важливою є духовна складова обороноздатності, яка включає патріотизм населення, моральний стан військовослужбовців, довіру громадян до державних інституцій, національну єдність, політичну стабільність та готовність суспільства до консолідованого спротиву агресору. Практика сучасних воєнних конфліктів, зокрема російської збройної агресії проти України, переконливо демонструє, що високий морально-психологічний рівень суспільства значною мірою визначає ефективність функціонування всієї системи національної оборони.

У сучасних умовах обороноздатність дедалі більше залежить від рівня цифрової трансформації сектору безпеки й оборони. Розвиток інформаційно-комунікаційних технологій, автоматизованих систем управління військами, безпілотних платформ, систем супутникового моніторингу, кібербезпеки та технологій штучного інтелекту формує новий технологічний вимір обороноздатності. Саме цифрові інновації забезпечують швидке ухвалення управлінських рішень, обробку великих масивів даних, прогнозування бойової обстановки, підвищення точності ураження цілей, автоматизацію логістичних процесів та оптимізацію використання оборонних ресурсів [6].

У цьому контексті особливого значення набуває система публічного управління, яка повинна забезпечувати ефективну координацію діяльності всіх суб'єктів сектору безпеки й оборони, формування державної політики у сфері оборони, розподіл ресурсів, нормативно-правове забезпечення, міжвідомчу взаємодію та інтеграцію сучасних цифрових технологій у процеси оборонного планування. Від ефективності управлінських механізмів значною мірою залежить здатність держави своєчасно адаптуватися до нових викликів і забезпечувати стале функціонування оборонної системи.

Саме тому, обороноздатність держави слід розглядати як багаторівневу інтегровану систему, що поєднує військові, економічні, технологічні, інформаційні, соціальні та управлінські компоненти, спрямовані на забезпечення національної безпеки та захист державного суверенітету. В умовах повномасштабної війни та стрімкого розвитку технологій ключовими чинниками підвищення обороноздатності стають цифровізація сектору безпеки і оборони, впровадження технологій штучного інтелекту, розвиток інноваційного оборонно-промислового комплексу та удосконалення механізмів публічного управління, що дає змогу забезпечити більш ефективне реагування на сучасні воєнні загрози.

Що стосується штучного інтелекту, то він безпосередньо може посилювати обороноздатність України за кількома основними напрямами.

Першим напрямом є розвідувально-аналітична діяльність. Технології штучного інтелекту дозволяють аналізувати супутникові знімки, відео з безпілотних літальних апаратів, відкриті джерела інформації, радіоелектронні дані, повідомлення в інформаційному просторі та інші масиви даних. Це дає змогу швидше виявляти загрози, ідентифікувати об'єкти, прогнозувати переміщення сил противника та підвищувати якість ситуаційної обізнаності [12].

Іншим напрямом є підтримка ухвалення управлінських і військових рішень. Системи штучного інтелекту можуть використовуватися для моделювання сценаріїв, оцінки ризиків, прогнозування наслідків рішень, оптимізації ресурсів і підвищення точності планування. У публічно-управлінському вимірі це означає посилення аналітичної спроможності органів державної влади та військового управління [10].

Третім напрямом є кібероборона. Штучний інтелект здатний виявляти аномальну активність у мережах, прогнозувати кіберзагрози, автоматизувати реагування на інциденти, аналізувати поведінку шкідливого програмного забезпечення та захищати критичну інформаційну інфраструктуру. Для України, яка системно зазнає кібератак, цей напрям має особливе значення.

Четвертим напрямом є розвиток безпілотних і автономних систем. Український досвід війни засвідчив надзвичайну роль безпілотних платформ у розвідці, коригуванні вогню, ураженні цілей, логістиці та моніторингу поля бою. Інтеграція штучного інтелекту в такі системи може підвищити їхню автономність, точність, стійкість до радіоелектронної боротьби та ефективність застосування.

П'ятим напрямом є оборонна логістика. Алгоритми штучного інтелекту можуть оптимізувати маршрути постачання, прогнозувати потреби у ресурсах, управляти запасами, визначати ризики логістичних затримок і підвищувати стійкість системи забезпечення військ.

Шостим напрямом є інформаційна безпека та протидія дезінформації. Штучний інтелект може використовуватися для виявлення інформаційних операцій, аналізу ворожої пропаганди, моніторингу соціальних мереж, ідентифікації бот-мереж і прогнозування інформаційних впливів [7].

Водночас потенціал штучного інтелекту не реалізується автоматично. Для його ефективного використання необхідні належні управлінські рішення, стабільне фінансування, кадровий потенціал, безпечна цифрова інфраструктура, доступ до якісних даних, міжвідомча координація, правове регулювання та система контролю. Саме тому питання використання штучного інтелекту у сфері оборони слід розглядати насамперед як проблему державної політики та публічного управління.

Публічно-управлінський вимір використання штучного інтелекту у сфері оборони полягає в тому, що держава має забезпечити цілісну систему управління цим процесом – від стратегічного бачення до практичної реалізації, моніторингу та оцінювання результатів. Без належної державної політики навіть найперспективніші технологічні рішення можуть залишатися фрагментарними, несумісними, недостатньо захищеними або неефективними.

Основними суб'єктами формування та реалізації державної політики у цій сфері є Верховна Рада України, Президент України, Кабінет Міністрів України, Міністерство оборони України, Міністерство цифрової трансформації України, Генеральний штаб Збройних Сил України, Рада національної безпеки і оборони України, інші органи сектору безпеки й оборони, наукові установи, заклади вищої освіти, підприємства оборонно-промислового комплексу, приватні технологічні компанії та громадянське суспільство.

У межах публічного управління держава має виконувати кілька ключових функцій (табл. 1).

Як свідчать дані таблиці 1, ефективне використання штучного інтелекту у сфері оборони неможливе без комплексної реалізації взаємопов'язаних функцій державного управління. Кожна із запропонованих

функцій охоплює окремий напрям державної політики, однак лише їх інтегроване застосування забезпечує створення цілісної системи управління цифровою трансформацією сектору безпеки та оборони.

Таблиця 1

Основні функції держави у сфері публічного управління використанням штучного інтелекту для підвищення обороноздатності України

№	Функція	Зміст функції	Практичне значення
1	**Стратегічна**	Формування державної політики щодо розвитку штучного інтелекту в оборонній сфері, визначення стратегічних цілей, пріоритетів, етапів реалізації та показників ефективності	Забезпечує довгостроковий розвиток оборонних технологій, узгодженість державної політики та ефективне стратегічне планування
2	**Нормативно-правова**	Розроблення законодавчої бази щодо створення, тестування, закупівлі, експлуатації та контролю систем штучного інтелекту, визначення відповідальності, вимог до захисту інформації та безпеки даних	Створює правові гарантії безпечного, прозорого та контрольованого використання технологій штучного інтелекту
3	**Інституційна**	Формування системи органів управління, визначення компетенції державних органів, координація міжвідомчої взаємодії, створення центрів компетенцій та експертних платформ	Забезпечує ефективне функціонування системи управління та координацію діяльності всіх учасників оборонного сектору
4	**Ресурсна**	Фінансування фундаментальних і прикладних досліджень, підтримка оборонних інновацій, стартапів, цифрової інфраструктури, модернізація технічного забезпечення та закупівля сучасних технологій	Створює матеріальну основу для розвитку оборонних інновацій та цифрової трансформації сектору безпеки і оборони
5	**Кадрова**	Підготовка, перепідготовка та підвищення кваліфікації фахівців у сфері штучного інтелекту, оборони, кібербезпеки, права, аналітики та публічного управління	Формує людський капітал, необхідний для ефективного використання сучасних цифрових технологій у секторі оборони

Джерело: складено автором

Визначальне місце у цій системі займає стратегічна функція, яка формує довгострокові орієнтири розвитку оборонної сфери та визначає пріоритети державної політики щодо впровадження технологій штучного інтелекту. Саме стратегічне планування забезпечує узгодження діяльності всіх органів державної влади, розподіл ресурсів та оцінювання результативності реалізації державних програм [10].

Не менш важливою є нормативно-правова функція, яка створює правове підґрунтя для функціонування систем штучного інтелекту. В умовах стрімкого розвитку цифрових технологій особливого значення набуває своєчасне вдосконалення законодавства, що регулюватиме питання відповідальності за прийняття автоматизованих рішень, захисту персональних даних, інформаційної безпеки, використання автономних систем озброєння та дотримання міжнародного гуманітарного права [11].

Водночас інституційна функція забезпечує організаційну спроможність держави реалізовувати визначену політику шляхом чіткого розподілу компетенції між органами державної влади, створення спеціалізованих центрів розвитку штучного інтелекту, налагодження міжвідомчої взаємодії та інтеграції наукових установ, оборонної промисловості й військових структур.

Важливим чинником успішної цифрової трансформації є ресурсна функція, яка передбачає належне фінансове забезпечення досліджень, інноваційних розробок, модернізації цифрової інфраструктури, розвитку оборонних стартапів і впровадження сучасних технологічних рішень. Без достатнього фінансування навіть найбільш перспективні проєкти у сфері штучного інтелекту не можуть бути реалізовані на практиці.

Особливого значення набуває кадрова функція, оскільки сучасні технології потребують висококваліфікованих спеціалістів, здатних поєднувати компетентності у сфері публічного управління, військової справи, інформаційних технологій, кібербезпеки, права та аналізу даних. Саме людський капітал стає ключовим ресурсом цифрової модернізації оборонного сектору.

Завершальним елементом є контрольна функція, яка забезпечує постійний моніторинг ефективності використання систем штучного інтелекту, аудит алгоритмів, оцінювання потенційних ризиків і запобігання можливим зловживанням. В умовах широкого використання автономних інформаційних систем саме державний контроль дозволяє гарантувати прозорість, підзвітність, безпечність та відповідність функціонування штучного інтелекту національному законодавству і міжнародним стандартам.

Отже, наведені функції формують комплексний механізм публічного управління розвитком і використанням штучного інтелекту у сфері оборони. Їхня реалізація сприятиме формуванню сучасної моделі державного управління, яка ґрунтуватиметься на стратегічному плануванні, міжвідомчій координації, цифровій трансформації, розвитку людського потенціалу та відповідальному використанні інноваційних технологій. У свою чергу, це створить передумови для підвищення обороноздатності України, зміцнення національної безпеки та забезпечення технологічної переваги держави в умовах сучасних воєнних викликів.

Висновки та перспективи подальших досліджень. У результаті проведеного дослідження встановлено, що використання технологій штучного інтелекту стає одним із визначальних напрямів модернізації сектору безпеки й оборони України та важливою складовою забезпечення обороноздатності держави. В умовах цифрової трансформації, розвитку гібридних загроз, кіберпростору як нового театру воєнних дій та широкого застосування автономних систем ефективність державної політики значною мірою залежить від здатності органів публічної влади інтегрувати інноваційні технології у процеси стратегічного планування, управління та оборонного забезпечення.

Обґрунтовано, що обороноздатність держави необхідно розглядати як багатокомпонентну систему, яка поєднує військові, економічні, технологічні, інформаційні, соціальні та управлінські складові. За таких умов штучний інтелект виступає не лише інструментом автоматизації окремих процесів, а й стратегічним ресурсом, здатним підвищити якість інформаційно-аналітичного забезпечення, оперативність ухвалення рішень, ефективність кібероборони, функціонування безпілотних систем, оборонної логістики та протидії інформаційним загрозам.

Доведено, що ефективне використання технологій штучного інтелекту потребує формування комплексної системи публічного управління, яка повинна ґрунтуватися на реалізації стратегічної, нормативно-правової, інституційної, ресурсної, кадрової та контрольної функцій держави. Лише їх взаємодія забезпечує створення належних організаційних, правових, фінансових і кадрових умов для масштабного впровадження інноваційних технологій у секторі безпеки й оборони.

Перспективними напрямами подальших наукових досліджень є розроблення механізмів державного регулювання використання генеративного штучного інтелекту та автономних бойових систем, удосконалення нормативно-правового забезпечення застосування технологій штучного інтелекту відповідно до міжнародних стандартів, а також формування моделей міжвідомчої координації та оцінювання ефективності державної політики у сфері цифрової трансформації сектору безпеки й оборони України.

Література.

1. ***Alon-Barkat, S., & Busuioc, M.*** (2021). Human-AI Interactions in Public Sector Decision-Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice. https://arxiv.org/abs/2103.02381

2. ***Kott, A., Théron, P., Drašar, M., Dushku, E., LeBlanc, B., Losiewicz, P., et al.*** (2018). Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. NATO Research Task Group IST-152. https://arxiv.org/abs/1803.10664

3. ***Théron, P., Kott, A., Drašar, M., Rzadca, K., LeBlanc, B., Pihelgas, M., et al.*** (2018). Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture. https://arxiv.org/abs/1806.08657

4. ***Harding, V.*** (2024). *AI Needs You: How We Can Change AI's Future and Save Our Own*. Princeton University Press. https://press.princeton.edu/books/hardcover/9780691244570/ai-needs-you

5. 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). *(2024).* Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

6. Council of Europe. (2024). *The Framework Convention on Artificial Intelligence*. Strasbourg. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

7. ***Савченко, В. А., & Шаповаленко, О. Д.*** (2020). Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації*, № 4(44), 6–11.

8. **Про оборону України.** (1991). (Закон України № 1932-XII від 6 грудня 1991 р.). https://zakon.rada.gov.ua/go/1932-12

9. ***Пустовіт, Я. Б., & Гбур, З. В.*** (2023). Використання штучного інтелекту в підвищенні обороноздатності України: аспекти публічного управління. *Інвестиції: практика та досвід*, № 13, 103–108. https://doi.org/10.32702/2306-6814.2023.13.103

10. ***Пустовіт, Я. Б., & Гбур, З. В.*** (2024). Аналіз існуючих стратегій у державному управлінні щодо використання штучного інтелекту в обороні. *Успіхи та досягнення в науці*, № 1(1), 172–185. https://doi.org/10.52058/3041-1254-2024-1(1)-172-185

11. ***Шумлянський, С. В., Хоменко, Є. В., & Попрієнко, С. В.*** (2025). Ризикоорієнтований підхід до впровадження штучного інтелекту у сфері оборони України: концептуальні засади. *Military Science*, 3(3), 147–161. The Central Research Institute of the Armed Forces of Ukraine. https://doi.org/10.62524/msj.2025.3.3.11

12. ***Краснов, Р. В., Шумлянський, С. В., & Світлічний, І. В.*** (2025). Використання штучного інтелекту у військовій галузі: ризики та загрози для особового складу. *Human Rights and Public Governance*. Scientific monograph. Riga, Latvia: Baltija Publishing, 356–376. https://doi.org/10.30525/978-9934-26-608-9-19

References.

1. ***Alon-Barkat, S., & Busuioc, M.*** (2021). Human-AI Interactions in Public Sector Decision-Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice. https://arxiv.org/abs/2103.02381

2. ***Kott, A., Théron, P., Drašar, M., Dushku, E., LeBlanc, B., Losiewicz, P., et al.*** (2018). Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. NATO Research Task Group IST-152. https://arxiv.org/abs/1803.10664

3. ***Théron, P., Kott, A., Drašar, M., Rzadca, K., LeBlanc, B., Pihelgas, M., et al.*** (2018). Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture. https://arxiv.org/abs/1806.08657

4. ***Harding, V.*** (2024). *AI Needs You: How We Can Change AI's Future and Save Our Own*. Princeton University Press. https://press.princeton.edu/books/hardcover/9780691244570/ai-needs-you

5. *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).* (2024). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

6. **Council of Europe.** (2024). *The Framework Convention on Artificial Intelligence*. Strasbourg. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

7. ***Savchenko, V. A., & Shapovalenko, O. D.*** (2020). *Osnovni napriamy zastosuvannia tekhnolohii shtuchnoho intelektu u kiberbezpetsi* [Main directions of application of artificial intelligence technologies in cybersecurity]. *Suchasnyi zakhyst informatsii* [Modern Information Protection], 4(44), 6–11.

8. *Pro oboronu Ukrainy* [On Defense of Ukraine]. (Law of Ukraine No. 1932-XII of December 6, 1991). https://zakon.rada.gov.ua/go/1932-12

9. ***Pustovit, Ya. B., & Hbur, Z. V.*** (2023). *Vykorystannia shtuchnoho intelektu v pidvyshchenni oboronozdatnosti Ukrainy: aspekty publichnoho upravlinnia* [The use of artificial intelligence to enhance Ukraine's defense capability: Aspects of public administration]. *Investytsii: praktyka ta dosvid* [Investments: Practice and Experience], (13), 103–108. https://doi.org/10.32702/2306-6814.2023.13.103

10. ***Pustovit, Ya. B., & Hbur, Z. V.*** (2024). *Analiz isnuiuchykh stratehii u derzhavnomu upravlinni shchodo vykorystannia shtuchnoho intelektu v oboroni* [Analysis of existing public administration strategies regarding the use of artificial intelligence in defense]. *Uspikhy ta dosiahnennia v nautsi* [Advances and Achievements in Science], 1(1), 172–185. https://doi.org/10.52058/3041-1254-2024-1(1)-172-185

11. ***Shumlianskyi, S. V., Khomenko, Ye. V., & Popriienko, S. V.*** (2025). *Ryzykooriientovanyi pidkhid do vprovadzhennia shtuchnoho intelektu u sferi oborony Ukrainy: kontseptualni zasady* [Risk-oriented approach to the implementation of artificial intelligence in the defense sector of Ukraine: Conceptual principles]. *Military Science*, 3(3), 147–161. https://doi.org/10.62524/msj.2025.3.3.11

12. ***Krasnov, R. V., Shumlianskyi, S. V., & Svietlichnyi, I. V.*** (2025). *Vykorystannia shtuchnoho intelektu u viiskovii haluzi: ryzyky ta zahrozy dlia osobovoho skladu* [The use of artificial intelligence in the military sphere: Risks and threats to military personnel]. *Human Rights and Public Governance* [Human Rights and Public Governance]. Riga, Latvia: Baltija Publishing. https://doi.org/10.30525/978-9934-26-608-9-19

Abstract.

Pustovit Y. State policy on the use of artificial intelligence technologies in the defense sphere of Ukraine.

The article examines the peculiarities of the formation of state policy regarding the use of artificial intelligence technologies as one of the key factors in strengthening Ukraine's defense capability under contemporary security challenges. It substantiates that the digital transformation of the security and defense sector necessitates a reconsideration of public administration approaches aimed at implementing innovative technologies, improving the effectiveness of managerial decision-making, and ensuring the state's technological superiority. The essence of state policy on the application of artificial intelligence in defense is revealed, and its main functions are identified, including information and analytical support, decision-making assistance, cyber defense, autonomous systems, defense logistics, and information security. The study analyzes contemporary approaches to understanding national defense capability and demonstrates that its effectiveness increasingly depends on the level of digitalization, technological development, cybersecurity resilience, and the efficiency of public administration. Particular attention is paid to identifying the key functions of the state within the framework of public administration of artificial intelligence technologies, namely strategic, regulatory, institutional, resource, human resource, and control functions. It is argued that the comprehensive implementation of these functions creates the necessary conditions for the effective integration of artificial intelligence technologies into the security and defense sector, promotes the development of defense innovations, strengthens national security, and enhances Ukraine's defense capability.

Keywords: *artificial intelligence, public administration, state policy, defense capability, security and defense sector, digital transformation, national security, cybersecurity, defense technologies.*

Стаття надійшла до редакції / Received 04.06.2026 Прийнята до друку / Accepted 16.06.2026 Опубліковано/ Published 08.08.2026

Бібліографічний опис статті:

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.

Pustovit Y. State policy on the use of artificial intelligence technologies in the defense sphere of Ukraine. Actual problems of innovative economy and law. 2026. No. 3, pp. 191-195.