УДК 004.89
DOI https://doi.org/10.32782/TNU-2663-6468/2024.6/21

Гриндей А.О.
Український науково-дослідний інститут спеціальної техніки
та судових експертиз Служби безпеки України

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОБОРОННІЙ СФЕРІ

У статті досліджено актуальність використання штучного інтелекту (ШІ) в оборонній сфері в контексті трансформації сучасного характеру воєнних конфліктів та зростання технологічної конкуренції між провідними державами світу. Розглянуто ключові напрями впровадження ШІ, зокрема автоматизацію збору, аналізу та обробки даних у військовій розвідці, що сприяє підвищенню швидкості та точності ухвалення рішень на полі бою. Особлива увага приділяється використанню ШІ для забезпечення кібербезпеки, запобігання кібератакам і захисту критично важливих інформаційних систем.

Детально описано роль автономних бойових систем, включаючи безпілотні літальні апарати, наземні та морські платформи, які здатні виконувати завдання з мінімальним втручанням людини. Розкрито можливості ШІ для оптимізації логістики, включаючи управління постачанням ресурсів, транспортуванням та підтримкою особового складу, що дозволяє значно зменшити витрати часу та ресурсів.

У статті проаналізовано ключові переваги впровадження ШІ в оборонні операції, такі як підвищення ефективності виконання завдань, зниження ризиків для особового складу, покращення точності прогнозування потенційних загроз та моделювання сценаріїв розвитку конфліктів. Окремо розглянуто виклики, які виникають у процесі інтеграції ШІ у військову сферу, серед яких складнощі із забезпеченням кіберзахисту систем ШІ, етичні дилеми, пов'язані з автономністю бойових рішень, та необхідність створення міжнародної нормативно-правової бази для регулювання використання ШІ у військових цілях.

Також визначено перспективи розвитку адаптивних систем управління боєм, які базуються на гіпермережевих технологіях, що забезпечують обмін інформацією між різними рівнями командування та підрозділами в режимі реального часу. Підкреслено важливість інструментів для моделювання та прогнозування воєнних конфліктів із використанням ШІ, які дозволяють краще розуміти динаміку загроз і знаходити оптимальні шляхи їх нейтралізації.

У статті обґрунтовано важливість комплексного підходу до інтеграції штучного інтелекту в оборонну сферу, який має враховувати не лише технічні аспекти, але й правові, соціальні та гуманітарні фактори. Зроблено висновок, що використання ШІ відкриває нові можливості для посилення обороноздатності держав, але потребує відповідального підходу з боку урядів, науковців та міжнародної спільноти.

Ключові слова: *штучний інтелект, оборонна сфера, автономні системи, кібербезпека, логістика.*

Постановка проблеми. Використання штучного інтелекту (ШІ) у сфері оборони набуває особливої актуальності в умовах стрімкого розвитку технологій та змін характеру сучасних воєнних конфліктів. Сьогодні оборонні стратегії провідних держав світу дедалі більше ґрунтуються на впровадженні інноваційних рішень, що забезпечують перевагу на полі бою. Штучний інтелект відіграє ключову роль у цій трансформації, сприяючи підвищенню ефективності управління ресурсами, розвідки, логістики та прийняття рішень в умовах обмеженого часу.

Зростає складність сучасних воєнних дій, що вимагає швидкого аналізу великих обсягів інформації. Штучний інтелект дозволяє значно скоротити час на обробку даних, забезпечуючи точність та оперативність у прийнятті стратегічних рішень. Це особливо важливо для систем раннього попередження, протиповітряної оборони та кібербезпеки, де від швидкості реакції залежить національна безпека.

Водночас інтеграція ШІ в оборонну сферу відкриває нові можливості для створення автономних бойових систем, які здатні виконувати завдання без участі людини. Такі системи підвищують ефективність ведення бойових дій, мінімізуючи ризик втрат серед особового складу. Однак ці технології також породжують етичні питання, пов'язані з контролем за використанням автономної зброї та відповідальністю за її дії.

Таким чином, актуальність впровадження штучного інтелекту в оборонній сфері визначається як потребою в технологічній перевазі, так і необхідністю адаптації до умов сучасних конфліктів, які стають дедалі більш залежними від технологій нового покоління. Це викликає необхідність ґрунтовного дослідження можливостей і обмежень таких технологій, а також формування міжнародних норм щодо їх використання.

Аналіз останніх досліджень і публікацій. Розвиток технологій ШІ досліджують як іноземні, так і вітчизняні науковці. Поняття ШІ вперше ввів американський вчений Дж. МакКарті ще в 1956 році. Він досліджував можливості навчання комп'ютера, що міг би самостійно навчатися, думати та самовдосконалюватися. Вченими-першопроходцями також були А. Тюрінг, Й. Бенджі, Д. Хілтон та Я. Лекун, В. Глушков. Їх науковий внесок в розвиток комп'ютерних технологій створив основу для сучасного розвитку ШІ. Нині проблеми ШІ, зокрема стратегії їхнього розвитку, досліджують такі науковці, як А. Агравал, С. Хойманн, Н. Зан, Е. Вільямс, К. Шваб, В. Бланууца, С. Васін, Я. Селянин, І. Соколов. Вітчизняними дослідниками, які присвячують свою увагу цим проблемам, є Г. Андрощук, О. Баранов, В. Гончарук, К. Єфремова, О. Івахненко, Л. Калужнін, О. Кухтенко, О. Костенко, О. Краковецький, О. Радутний, О. Піжук, О. Пістракевич, В. Скурицін, В. Хаустова, А. Шевченко та ін.

Постановка завдання. Мета статті – дослідити сучасні напрями використання штучного інтелекту в оборонній сфері, оцінити його вплив на ефективність військових операцій, ідентифікувати ключові переваги, виклики та перспективи впровадження, а також обґрунтувати необхідність комплексного підходу до інтеграції ШІ з урахуванням етичних, правових та соціальних аспектів.

Виклад основного матеріалу. У галузі військової розвідки ШІ використовується для аналізу даних з різних джерел, зокрема супутникових знімків, радіолокаційної інформації та електронного спостереження. Завдяки машинному навчанню та алгоритмам обробки великих обсягів даних, штучний інтелект дозволяє ідентифікувати потенційні загрози ще на ранніх стадіях, прогнозувати розвиток ситуації та забезпечувати командуванню оперативні рекомендації. Це особливо важливо в умовах асиметричних конфліктів, де дії противника часто є непередбачуваними.

Кібербезпека також є важливим компонентом сучасної оборонної стратегії, де ШІ використовується для виявлення, аналізу та нейтралізації кібератак. Системи, оснащені штучним інтелектом, здатні не лише розпізнавати вже відомі загрози, але й виявляти нові, раніше невідомі моделі атак. Це значно підвищує рівень захищеності критично важливої інфраструктури, а також забезпечує стабільність роботи систем командування та управління [2].

Автономні бойові системи, зокрема безпілотні літальні апарати, наземні транспортні засоби та морські дрони, є ще одним прикладом впровадження штучного інтелекту. Ці технології дозволяють виконувати складні бойові завдання без безпосередньої участі людини, зменшуючи ризик втрат серед військовослужбовців. Крім того, автономні системи здатні працювати у важкодоступних або небезпечних зонах, таких як зони радіоактивного чи хімічного забруднення.

Важливим аспектом є також логістична підтримка, де ШІ використовується для оптимізації транспортних маршрутів, управління запасами та прогнозування потреб. Це дозволяє значно скоротити витрати на забезпечення військових операцій та підвищити їхню ефективність. Наприклад, автоматизовані системи управління можуть визначати найбільш оптимальні шляхи доставки боєприпасів чи гуманітарної допомоги у зону бойових дій, враховуючи зміну ситуації в реальному часі [5].

Попри численні переваги, впровадження ШІ в оборонну сферу супроводжується певними викликами. Серед них – необхідність забезпечення кіберзахисту самих систем ШІ, уникнення технічних збоїв, етичні дилеми, пов'язані із застосуванням автономної зброї, а також правові питання щодо відповідальності за її використання. Це потребує розробки чітких нормативно-правових актів, що регулюватимуть застосування таких технологій як на національному, так і міжнародному рівнях.

Отже, штучний інтелект у військовій сфері є не лише інструментом для підвищення ефективності оборонних можливостей, а й чинником, що змінює саму природу сучасних конфліктів. Його впровадження потребує комплексного підходу, що враховує як технологічні, так і соціально-етичні аспекти [4].

Подальший розвиток штучного інтелекту у військовій сфері залежить не лише від технологічних інновацій, але й від політичної волі та міжнародної співпраці. Одним із ключових викликів залишається забезпечення балансу між необхідністю використання новітніх технологій для забезпечення національної безпеки та дотриманням між-

народних норм гуманітарного права. Особливу увагу слід приділити розробці механізмів контролю за застосуванням автономних систем озброєнь, оскільки їхнє масове впровадження може призвести до непередбачуваних наслідків.

У науковій спільноті активно обговорюється питання розробки глобальних стандартів для використання ШІ у військових цілях. До таких стандартів можуть належати заборона на створення повністю автономної зброї, яка здатна приймати рішення про знищення без участі людини, вимоги до прозорості алгоритмів, що використовуються в бойових системах, а також заходи щодо запобігання поширенню цих технологій до держав чи організацій, які можуть використовувати їх у терористичних або агресивних цілях.

Окремо слід розглядати аспекти кібербезпеки у застосуванні ШІ. Залежність сучасних військових систем від алгоритмів штучного інтелекту створює нові вразливості, які можуть бути використані противником. Кібератаки, спрямовані на злам систем ШІ, можуть мати катастрофічні наслідки, особливо якщо вони впливають на системи управління озброєннями або стратегічними ресурсами. Тому розвиток технологій захисту, таких як алгоритми самонавчання, здатні адаптуватися до нових загроз, є важливим напрямом досліджень [1].

Необхідно враховувати потенціал подвійного призначення технологій ШІ. Інновації, розроблені для оборонної сфери, можуть знайти застосування у цивільних галузях, таких як охорона здоров'я, транспорт чи енергетика. Наприклад, алгоритми аналізу великих даних, створені для розвідки, можуть бути адаптовані для моніторингу епідеміологічних ситуацій або запобігання природним катастрофам. Такий підхід сприятиме формуванню більш позитивного іміджу оборонних інновацій у суспільстві та стимулюватиме фінансування наукових досліджень.

У майбутньому очікується подальша інтеграція штучного інтелекту з іншими передовими технологіями, такими як квантові обчислення, блокчейн або біотехнології. Така синергія може кардинально змінити спосіб ведення бойових дій, роблячи їх більш точними, безпечними та прогнозованими. Проте це також вимагатиме відповідного перегляду існуючих концепцій військової стратегії, етики та міжнародного права.

Таким чином, дослідження використання штучного інтелекту в оборонній сфері є важливим кроком до розуміння його потенціалу, ризиків та необхідності регулювання. Комплексний підхід до впровадження цих технологій дозволить не лише підвищити обороноздатність, але й забезпечити їхнє використання відповідно до принципів гуманності та міжнародної безпеки.

У перспективі роль штучного інтелекту в оборонній сфері ставатиме дедалі важливішою, оскільки технологічний прогрес відкриває нові горизонти для створення адаптивних і автономних систем. Водночас інтеграція ШІ в усі етапи військової діяльності – від стратегічного планування до тактичних операцій – висуває серйозні вимоги до модернізації інфраструктури, систем управління та підготовки кадрів [3].

Одним із ключових напрямів майбутніх досліджень є розробка адаптивних систем управління боєм. Це системи, здатні оперативно аналізувати бойову обстановку, враховувати мінливі чинники й забезпечувати командирів достовірними даними для прийняття рішень. Удосконалення таких систем сприятиме зниженню навантаження на людський фактор, водночас залишаючи за людиною остаточний контроль над використанням озброєнь. Подібні рішення вже застосовуються у вигляді командно-штабних платформ, однак їхня ефективність значно зросте з удосконаленням ШІ.

Ще одним перспективним напрямом є розвиток гіпермережевих систем – поєднання бойових одиниць, безпілотних систем і сенсорів у єдину інформаційну мережу. Використання ШІ в таких системах дозволяє автоматично координувати дії різнорідних компонентів, забезпечуючи максимальну точність і злагодженість операцій. Наприклад, під час спільної роботи літаків, наземної техніки та безпілотників, штучний інтелект може самостійно розподіляти завдання, обирати найкращі маршрути та враховувати загрози, знижуючи ризики втрат.

Особливу увагу варто приділити ролі ШІ в прогнозуванні та моделюванні сценаріїв конфліктів. Сучасні технології дозволяють аналізувати величезні обсяги даних для моделювання можливих конфліктів із урахуванням політичних, економічних та військових чинників. Це допомагає прогнозувати не лише ймовірність виникнення конфлікту, але й його можливі наслідки. Наприклад, алгоритми аналізу великих даних уже використовуються для визначення ризиків регіональної ескалації на основі економічних санкцій чи переміщення військових сил.

У контексті національної безпеки важливим стає підготовка військових кадрів до роботи з інноваційними системами. Це передбачає зміну

підходів до навчання та створення нових освітніх програм, орієнтованих на освоєння ШІ, кібербезпеки та технологій автоматизації. Також потребується підготовка спеціалістів із етичних та правових питань, адже використання автономних систем озброєнь створює нові виклики в рамках міжнародного гуманітарного права.

Важливо наголосити, що використання ШІ у військовій сфері є не лише інструментом досягнення тактичної переваги, але й може слугувати засобом стримування. Наявність високотехнологічних оборонних систем, оснащених ШІ, може зменшувати ймовірність агресії з боку потенційних супротивників, забезпечуючи стабільність і баланс сил.

Висновки. Отже, інтеграція штучного інтелекту в оборонну сферу є комплексним і багатогранним процесом, що вимагає врахування технологічних, етичних, правових і соціальних аспектів. Вона має потенціал не лише трансформувати способи ведення війни, але й стати важливим інструментом у забезпеченні глобальної безпеки. Завдяки всебічним дослідженням та узгодженню міжнародних підходів до регулювання застосування ШІ можна створити безпечний та ефективний інструмент для забезпечення стабільності у світі.

Список літератури:

1. 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#Text (дата звернення: 20.11.2024).

2. Український інститут науково-технічної експертизи та інформації: Державна наукова установа. Електронний ресурс. URL: http://www.uintei.kiev.ua/ (дата звернення: 20.11.2024).

3. Енциклопедія кібернетики / відпов. ред. Глушков В. М. Т. 2 (М–Я). К. : Вид-во УРЕ, 1973. 576 с.

4. Про оборону України: Закон України від 06.12.1991 р. №1932-XII. URL: https://ips.ligazakon.net/ document/ view/t193200?an=1&ed=2023_03_21 (дата звернення: 20.11.2024).

5. Про розвідувальні органи України: Закон України від 22.03.2001 р. № 2331-III. URL: https://ips.ligazakon.net/ document/view/t012331?an=ul-120&ed=2008_06_03 (дата звернення: 20.11.2024).

6. Public administration and the protection of private rights: questioning its recognition and application under Ukrainian law / O. Brusakova, O. Karmaza, V. Vasylenko, V. Moroz – Ius Humani, Revista de Derecho, 2022. Журнал Ius Humany. Law Journal. Випуск 11(1) С. 29–418.

7. Modern tools for preventing self-destructive and suicidal behavior of minors using information technology / Moroz Vita. Philosophy, Economics and Law Review. Volume 2, no. 1, 2022. 212–222.

Hryndei A.O. USE OF ARTIFICIAL INTELLIGENCE IN THE DEFENSE SPHERE

The article examines the relevance of the use of artificial intelligence (AI) in the defense sphere in the context of the transformation of the modern nature of military conflicts and the growth of technological competition between the world's leading states. The key areas of AI implementation are considered, in particular, the automation of data collection, analysis and processing in military intelligence, which contributes to increasing the speed and accuracy of decision-making on the battlefield. Special attention is paid to the use of AI to ensure cyber security, prevent cyber attacks and protect critical information systems.

The role of autonomous combat systems, including unmanned aerial vehicles, land and sea platforms, that are capable of performing missions with minimal human intervention is described in detail. The possibilities of AI to optimize logistics, including the management of resource supply, transportation and personnel support, are revealed, which allows you to significantly reduce the costs of time and resources.

The article analyzes the key advantages of implementing AI in defense operations, such as increasing the efficiency of task performance, reducing risks for personnel, improving the accuracy of forecasting potential threats and modeling conflict scenarios. The challenges that arise in the process of integrating AI into the military sphere are separately considered, including difficulties with ensuring cyber protection of AI systems, ethical dilemmas related to the autonomy of combat decisions, and the need to create an international legal framework to regulate the use of AI for military purposes.

Prospects for the development of adaptive battle management systems based on hyper-network technologies, which ensure the exchange of information between different levels of command and units in real time, are also determined. The importance of tools for modeling and forecasting military conflicts with the use of AI, which allow to better understand the dynamics of threats and find optimal ways to neutralize them, is emphasized.

The article substantiates the importance of a comprehensive approach to the integration of artificial intelligence in the defense sphere, which should take into account not only technical aspects, but also legal, social and humanitarian factors. It was concluded that the use of AI opens up new opportunities for strengthening the defense capabilities of states, but requires a responsible approach on the part of governments, scientists and the international community.

Key words: *artificial intelligence, defense sphere, autonomous systems, cyber security, logistics.*