DOI: https://doi.org/10.26642/sas-2025-3(9)-48-55
УДК 355.45

Півненко Олександр
кандидат наук з державного управління
Головне управління Національної гвардії України
https://orcid.org/0009-0009-3528-609X

Гладков Вадим
Головне управління Національної гвардії України
https://orcid.org/0009-0001-3705-1974

Бєлай Сергій
доктор наук з державного управління, професор
Національна академія Національної гвардії України
https://orcid.org/0000-0002-0841-9522

Скляр Максим
Головне управління Національної гвардії України
https://orcid.org/0009-0004-3335-3774

Походенко Дмитро
ОЗБССП «Тайфун»
https://orcid.org/0009-0005-0183-3500

Обґрунтування концептуальних напрямів упровадження штучного інтелекту для потреб сектору безпеки і оборони України

Анотація. Досліджено питання обґрунтування концептуальних напрямів упровадження штучного інтелекту для потреб сектору безпеки і оборони України. Встановлено, що, попри широкий спектр дослідження питання розвитку і застосування штучного інтелекту у сфері безпеки і оборони, у наукових працях не приділено достатньої уваги вивченню саме концептуальних аспектів його упровадження для потреб сектору безпеки і оборони, що й зумовлює актуальність обраного напряму наукового дослідження. Метою статті є поглиблене вивчення питання використання штучного інтелекту у сфері функціонування складових сектору безпеки і оборони та обґрунтування відповідних концептуальних напрямів його впровадження. Для створення загальнодержавної (відомчої, міжвідомчої) платформи штучного інтелекту, особливо в контексті безпеки й оборони, запропоновано підхід «Наука – Розроблення – Використання». Доведено, що цей підхід сприяє забезпеченню системності, прозорості та ефективності на кожному етапі, дає змогу уникнути технократичних або ізольованих рішень, які не відповідають реальним викликам. Обґрунтовано, що сили оборони є ключовим стейкхолдером, проте ефективна державна платформа штучного інтелекту не може бути створена виключно у військовому середовищі. Зазначено, що залучення цивільних розробників, науковців та незалежних експертів підвищує якість ухвалення рішень. Штучний інтелект має «працювати» на оборону, але створюватися у співпраці з науковцями, цивільними технологічними компаніями та підрозділами Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, а також підприємствами Оборонно-промислового комплексу України.

Ключові слова: штучний інтелект; державна безпека; сектор безпеки і оборони; концептуальні напрями; послідовність упровадження; платформа.

Актуальність теми. Штучний інтелект (ШІ) стає ключовою технологією в сучасному світі, зокрема у сфері безпеки і оборони. Концепцією розвитку штучного інтелекту в Україні визначено, що у сфері оборони слід забезпечити використання технологій штучного інтелекту у системах: командування та управління; озброєння та військової техніки; збирання й аналізу інформації під час ведення бойових дій; аналізу / розвідки, підтримання й проведення розвідувальних заходів, оброблення картографічної

© Півненко О., Гладков В., Бєлай С., Скляр М., Походенко Д., 2025

інформації; протидії кіберзагрозам у сфері оборони, що базуються на застосуванні технологій штучного інтелекту, зокрема таких, які дають змогу швидко виявити кібератаки, попереднє сканування та наступне уникнення шкідливих кодів або сканування підозрілих моделей поведінки, а не конкретного коду; імітаційного та когнітивного моделювання бойової обстановки; когнітивного аналізу спроможностей військових підрозділів [1].

Застосування ШІ охоплює широкий спектр завдань: від оброблення великих обсягів інформації, розвідки й автономного управління до медичної і психологічної допомоги та кіберзахисту. Сьогодні ШІ є інструментом підтримання, а не заміною людського судження, його відповіді є лише відправною точкою для подальшого аналізу. Будь-яка система ШІ разом з великими мовними моделями (LLM) не дає однозначно правильних відповідей, а тільки генерує результат на основі ймовірнісної оцінки того, що є найбільш доречним або ймовірним у конкретному контексті. Це означає, що навіть, коли відповідь здається переконливою, вона не гарантує достовірності чи повноти.

Отже, будь-який результат, отриманий від ШІ, слід розглядати як чернетку, тобто початкову версію, яку необхідно допрацьовувати, перевіряти й адаптувати до конкретних умов, цілей чи стандартів. Людина, що користується ШІ, несе відповідальність за фінальне редагування, критичне мислення та прийняття рішень. Розуміння цього дає змогу уникати сліпої довіри до результату, зважаючи на фактори, які ШІ може не врахувати, а також забезпечувати точність, етичність та відповідність реальному контексту.

Аналіз останніх досліджень і публікацій. Питанням дослідження технологій використання ШІ у сфері безпеки і оборони приділяло увагу чимало дослідників і практиків. Так авторами статті [2] проведено аналіз використання штучного інтелекту у сфері забезпечення державної безпеки, зокрема у правоохоронній сфері, а саме запропоновано обґрунтовані рекомендації щодо вдосконалення нормативно-правової бази стосовно відповідальності, захисту персональних даних, кібербезпеки та етичного використання інструментарію ШІ. У праці [3] досліджено вплив штучного інтелекту на сучасні бойові дії та встановлено, що в умовах швидкого технологічного прогресу й дедалі більшої залежності збройних сил від нових технологій штучний інтелект стає важливим інструментом у стратегічному плануванні й тактичному виконанні операцій. Стратегічний концепт штучного інтелекту як радикальної інновації для цілей безпеки і оборони розкрито у дослідженні [4], а саме узагальнено формування тенденцій і рівень інноваційності його використання для цілей і завдань оборони за практикою провідних армій світу. У статті [5] акцентовано увагу на виявленні шляхів поліпшення результатів військових ігор завдяки впровадженню штучного інтелекту. Також визначено, що людино-машинна співпраця має потенціал для реалізації якісних досягнень у прийнятті рішень і може посилити навчання учасників, надаючи їм розуміння чинників, які дають змогу штучному інтелекту визначати найкращі варіанти і пов’язані з ними ризики. У праці досліджено сучасні умови технічної діяльності Збройних Сил України, що супроводжуються першочерговим і швидким реагуванням на загрози, а також ухваленням управлінських рішень на рівні командування та на рівні держави щодо забезпечення етапів ведення бойових дій [6]. У статті визначено роль і значення технологій ШІ у військово-технічній сфері [7], а саме: окреслено засади використання технологій штучного інтелекту у діяльності збройних сил; акцентовано увагу на загрозах і ризиках, які несе його використання у військово-технічній сфері; висвітлено особливості законодавчого забезпечення армійського використання технологій штучного інтелекту у США.

Отже, незважаючи на широкий спектр дослідження щодо розвитку і застосування ШІ у сфері безпеки і оборони, вивченню саме концептуальних аспектів його упровадження для потреб сектору безпеки і оборони в наукових працях не приділено достатньої уваги, що й зумовлює актуальність обраного напряму наукового дослідження.

Метою статті є поглиблене вивчення питання використання штучного інтелекту у сфері функціонування складових сектору безпеки і оборони та обґрунтування відповідних концептуальних напрямів його впровадження.

Викладення основного матеріалу. Для створення загальнодержавної (відомчої, міжвідомчої) платформи штучного інтелекту, особливо в контексті безпеки й оборони, критично важливо дотримуватися обґрунтованої послідовності «Наука – Розроблення – Використання». Такий підхід сприяє забезпеченню системності, прозорості та ефективності на кожному етапі, дає змогу уникнути технократичних або ізольованих рішень, які не відповідають реальним викликам. Доцільно виділити такі основні етапи наведеного підходу.

Eman I. Вивчення процедури розподілу обов’язків.

На цьому етапі основну роль відіграють академічні установи, які розробляють фундаментальні і прикладні моделі, етичні та правові межі, проводять дослідження у сфері оброблення даних, безпеки та людино-машинної взаємодії. Аналітичні центри також здійснюють оцінювання потенційного впливу ШІ на воєнну і цивільну сфери, моделювання сценаріїв використання.

Головним завданням цього етапу є створення наукової основи для системи, визначення принципів, обмежень, вимог до даних та допустимих рівнів автономності. До цього залучаються: цивільні технологічні компанії для реалізації моделей, інтерфейсів, інфраструктури, тестування систем у різних

сценаріях; інженерні підрозділи при Міністерстві оборони України та Оборонно-промисловому комплексі України для інтеграції у наявну військову інфраструктуру, перевірки відповідності стандартам безпеки та сумісності з існуючими системами; координаційні органи для управління проєктом, розподілу обов'язків та забезпечення відповідності цілям.

Важливим завданням є перетворення наукової ідеї на життєздатне рішення, що може масштабуватися й адаптуватися до динамічних потреб оборонної сфери. Отже, відбувається інтеграція у бойові та управлінські процеси. За цих обставин ключовими стейкхолдерами є: військові підрозділи як кінцеві користувачі платформи, які впроваджують рішення в реальному середовищі; інструктори і навчальні центри, де здійснюється підготовка кадрів до ефективного і відповідального використання ШІ; оператори й аналітики, які здійснюють взаємодію із системою, приймають рішення на основі даних, отриманих від ШІ. Крім того, важливим є забезпечення ефективного застосування технології у бойових умовах з урахуванням людського фактора, а також контролю та відповідальності.

Переваги такої моделі вбачаються: у цілісності (чіткий розподіл ролей і відповідальності); у гнучкості (можливості швидко адаптувати або поліпшувати систему завдяки відкритому цивільному компоненту й оперативній взаємодії між командами науковців, розробників та військових спеціалістів); у контролі якості (багаторівнева валідація на кожному етапі).

Eman II. Здійснення огляду напрямів ШІ та їх особливостей.

Різні типи ШІ мають свої функціональні задачі, методи побудови та вимоги до реалізації, а саме:

1) LLM (Large Language Models): генерація тексту, підтримання рішень, аналіз документів (побудова потребує використання трансформерних архітектур, потужних GPU-кластерів та високоякісних текстових корпусів);

2) Computer Vision (CV): автоматичне виявлення об'єктів, сегментація зображень, розпізнавання сцен (необхідні анотації, супутникові або аерофотознімки, а також спеціалізовані фахівці (CV Engineers, GIS Analysts));

3) аналіз даних і прогнозування, а саме виявлення аномалій, поведінковий аналіз, прогноз ризиків (використовуються класичні моделі машинного навчання, time series аналіз, graph-based AI);

4) робототехніка й автономні системи (дрони, наземні платформи): навігація, SLAM, управління груповою поведінкою (залучаються фахівці з робототехніки, сенсорики, вбудованих систем);

5) кіберзахист (виявлення атак, побудова захищених систем, реагування на інциденти);

6) інформаційні і психологічні операції (ASR, TTS, NER): розпізнавання і синтез мовлення, оброблення текстів, переклад (залучаються інженери з аудіо-аналізу та оброблення мови);

7) Edge AI (реалізація моделей на мікроконтролерах і вбудованих пристроях, робота без інтернету);

8) генеративний ШІ (створення зображень, текстів, відео для симуляцій або інформаційно-психологічних операцій);

9) ШІ для систем управління (підтримання прийняття рішень, інтеграція розвідданих, моделювання сценаріїв);

10) медичний і психологічний ШІ (дистанційна діагностика, автоматичний тріаж, допомога у випадках поранень та психологічних проблем).

Розглянемо основні приклади застосування різних типів ШІ за представленою класифікацією (табл. 1).

Таблиця 1

Основні приклади застосування різних типів ШІ

Напрям	Пояснення	Приклади застосування
1	2	3
1. Оброблення природної мови		
LLM (Large Language Models)	Моделі, що розуміють і генерують текст	Генерація чернеток документів, чат-боти
Machine Translation	Автоматичний переклад текстів та аудіо	Переклад інструкцій, інтерфейсів, документів
Speech Recognition (ASR)	Розпізнавання мовлення з аудіо	Конвертація аудіозапису в текст, субтитри
Text-to-Speech (TTS)	Генерація мови з тексту	Голосові помічники, відтворення мовлення команд
Speech-to-Speech (S2S)	Переклад усної мови в реальному часі	Тактичний переклад між військовими союзниками

Продовження табл. 1

1	2	3
Text Classification	Класифікація документів, текстів	Виявлення фейків, пропаганди, аналіз інфополів, оцінювання рівня секретності, виявлення продуктів витоків інформації
Named Entity Recognition (NER)	Виявлення осіб, місць, об'єктів у тексті	Розвідка, розбір повідомлень противника
2. Комп'ютерний зір		
Object Detection	Виявлення об'єктів на зображеннях / відео	Виявлення техніки, людей, дронів
Image Classification	Визначення класу зображення	Автоматична ідентифікація типу техніки
Facial Recognition	Розпізнавання облич	Скринінг, ідентифікація підозрюваних, перевірка особи
Scene Understanding	Аналіз ситуації в кадрі	Аналіз бою, кількість об'єктів, напрямок руху
Segmentation	Поділ зображення на кластери	Військове картографування, аналіз ландшафту
OCR (Optical Character Recognition)	Розпізнавання тексту на фото	Оброблення документів, номерів техніки
Night Vision AI	Оброблення ІЧ / теплових зображень	Поліпшення нічної видимості
3. Аналітика даних / Прогнозування		
Predictive Analytics	Прогнозування майбутніх подій	Планування логістики, передбачення атак
Anomaly Detection	Виявлення аномалій	Кібербезпека, розвідка
Recommendation Systems	Системи рекомендацій	Пропозиція рішень командиру
Multi-agent Simulation	Моделювання бойових сценаріїв	Симуляція бою, логістики, дій супротивника
4. Робототехніка та автономні системи		
Autonomous Navigation	Частково автономне пересування (автопілот, що його можна увімкнути / вимкнути)	Дрони, наземні платформи
SLAM (Simultaneous Localization and Mapping)	Одночасна побудова карти і позиціонування	Наземні БПЛА, сапери
Swarm Intelligence	Координація груп дронів	Масовані атаки FPV, розвідка
HRI (Human-Robot Interaction)	Взаємодія людини з автономною системою	Напівавтономні роботи-сапери, екзоскелети
5. Кіберзахист		
Threat Detection	Виявлення атак, вторгнень	Захист інфраструктури
User Behavior Analytics	Аналіз поведінки користувачів	Виявлення шпигунів
Automated Response Systems	Автоматичні реакції на атаки	ШІ-захист серверів
AI-driven Honeypots	Інтелектуальні пастки для хакерів	Контррозвідка в кіберпросторі
6. Інформаційні та психологічні операції		
Fake News Detection	Виявлення фейкових новин	Аналіз соцмереж, Телеграм-каналів
Sentiment Analysis	Аналіз емоційного тону	Моніторинг громадської думки

Закінчення табл. 3

1	2	3
Influence Operations Modeling	Моделювання кампаній впливу	Захист від інформаційних атак
Generative Content (Images, Text)	Створення інфо-матеріалів	Стратегічні комунікації, відео / фото
7. Робота на мікроконтролерах і вбудованих пристроях, робота без інтернету		
Low-power AI on microcontrollers	ШІ на малопотужних пристроях	Дрони, сенсори, радіостанції
Offline AI models	Робота без доступу до інтернету	Тактичні умови, БПЛА
Federated Learning	Навчання моделей без централізації даних	БПЛА, польові системи
8. Генеративний ШІ		
Text Generation	Генерація текстів	Протоколи, фейкові повідомлення
Image / Video Generation	Створення зображень, deepfake	Інформаційні і психологічні операції, симуляції
Data Augmentation	Генерація навчальних даних	Поліпшення точності моделей
9. Управління бойовими діями		
AI-assisted Decision Making	Підтримка командирів у прийнятті рішень	Прогноз ризиків, підбір варіантів дій
Sensor Fusion	Об’єднання даних з різних джерел	Агрегування розвідувальних даних
Mission Planning AI	Планування операцій	Автоматичний маршрут, координація підрозділів
10. Медицина, психологія та евакуація		
AI for Diagnostics	Автоматична діагностика	Перевірка поранених у польових умовах, психологічна допомога
Medical Prioritization (Triage AI)	Визначення черговості надання допомоги	Автоматичне оцінювання тяжкості поранень
Autonomous Evacuation Drones	Евакуація поранених без людини	Транспортування у зонах вогню

Етап III. Обґрунтування інфраструктурних вимог у частині централізованих та децентралізованих рішень.

Серед ключових складнощів реалізації – отримання достатніх обсягів якісних даних для навчання моделей; високі обчислювальні вимоги; збирання, оброблення, зберігання великих і конфіденційних наборів даних; етичні та юридичні аспекти (особливо у контексті автономного ураження цілей); забезпечення надійності, масштабованості та кіберстійкості систем. Інфраструктурні вимоги: централізовані і децентралізовані рішення.

Централізована інфраструктура (на рівні відомча / міжвідомча / державна платформи ШІ) містить:

– GPU / TPU сервери (кластер із сотнями відеокарт класу A100 / H100);
– Data Lake / warehouse на десятки петабайт;
– Kubernetes / VM для масштабування моделей та сервісів;
– захищений VPN / Zero Trust доступ для користувачів;
– механізми авторизації, багаторівневий контроль доступу та постійна технічна підтримка.

До складу децентралізованої системи (edge / польові рішення) входять:

– вбудовані пристрої (Jetson, Raspberry Pi, OAK-D, STM32);
– прискорені моделі (ONNX, TensorRT, quantized PyTorch);
– радіозахищені канали передачі даних;
– периферійне зберігання і локальне оброблення;
– адаптація до польових умов (пил, тепло, нестабільне живлення).

У таблиці 2 наведено порівняння типів рішень, які можуть використовуватися у централізованій та децентралізованій системах.

Таблиця 2

Порівняння типів рішень централізованої і децентралізованої систем

Критерій	Централізована система	Децентралізована система
Швидкість упровадження	Повільна (через складну систему захисту інформації)	Швидка (масштабування у разі потреби)
Масштабованість	Висока (у разі правильної архітектури)	Потребує налаштування і моніторингу вузлів
Кіберзахист	Централізоване оновлення	Ризик втрати контролю над пристроями
Юридичний контроль	Простіше регламентувати	Ускладнене дотримання процедур
Надійність	Єдина точка відмови у разі DDoS /вторгнення	Надмірність, але складна синхронізація
Вартість	Висока CAPEX (дата-центри, сертифікація)	Велика маса пристроїв, заміна, живлення

З огляду на порівняння типів рішень централізованої і децентралізованої систем отримуємо гібридний підхід – архітектуру, що поєднує обчислювальні можливості і стандарти централізованої державної / відомчої платформи із гнучкістю локального розроблення й автономного функціонування польових систем. Ключовою особливістю такого підходу є те, що він дає змогу централізовано формувати загальні стандарти, API, навчальні моделі та безпекову політику, водночас підтримуючи гнучке розроблення проєктів локальними командами, які працюють у різних доменах (розвідка, логістика, FPV, зв'язок тощо), але в узгоджених архітектурних межах.

Отже, система може масштабуватися горизонтально (через розгортання edge-рішень), вертикально (через централізовані сервіси) та організаційно (завдяки делегуванню ініціатив командам, що працюють над конкретними бойовими завданнями). Це дає змогу підвищити інноваційність, оперативність та адаптивність оборонних рішень, не поступаючись цілісністю, кібербезпекою та стратегічною сумісністю.

Eman IV. Розрахунок юридичних і нормативних викликів.

Основними проблемами сфери юридичних і нормативних викликів є:

– відсутність специфічного законодавства для ШІ в обороні (крім загальних вимог законів України «Про захист інформації», «Про державну таємницю», а також ДСТУ);

– правове регулювання автономних рішень (наприклад, ураження цілей ШІ без прямої участі людини є потенційним порушенням міжнародного гуманітарного права);

– питання відповідальності (хто несе відповідальність у випадку помилкових рішень моделі?);

– персональні дані (збирання, оброблення та зберігання даних військовослужбовців і цивільних осіб);

– контроль за експортом / імпортом ШІ-рішень (деякі алгоритми чи моделі підпадають під обмеження, наприклад генерація deepfake).

Eman V. Створення комплексної системи захисту інформації.

Комплексна система захисту інформації є обов'язковою вимогою для державних інформаційних систем, які обробляють: службову інформацію, персональні дані, конфіденційну інформацію, відомості з обмеженим доступом.

Основними елементами комплексної системи захисту інформації є: 1) політика безпеки, модель загроз; 2) аутентифікація / авторизація; 3) журнали подій, контроль доступу; 4) криптозахист, сертифіковані засоби; 5) сертифікація Державною службою спеціального зв'язку та захисту інформації України.

Структуру безпекового профілю системи ШІ наведено у таблиці 3.

Таблиця 3

Структура безпекового профілю системи ШІ

Компонент	Централізована система	Децентралізована система
Типи загроз	Атаки на інфраструктуру, централізований доступ	Компрометація окремих вузлів, фізичний доступ
Рівень контролю	Високий (централізована політика)	Низький (ускладнений аудит)
Криптозахист	TLS, VPN, сертифікати	Вбудовані протоколи, light-weight TLS
Журнали / аудит	Централізовані SIEM-системи	Локальні, можливо із синхронізацією
Доступ / ідентифікація	RBAC, SSO, КЕП	Token-based, biometric, QR + pin
Захист даних	Сховище з backup, шифрування	Локальний з шифруванням, епізодичний backup
Фізичний захист	Централізований захист інфраструктури	Польові умови, захищені корпуси пристроїв

Висновки та перспективи подальших досліджень. Розгортання і використання штучного інтелекту в секторі безпеки і оборони – це не лише технологічне оновлення, а й фундаментальна трансформація способу ведення бойових дій, аналізу інформації та ухвалення рішень. Штучний інтелект дає змогу досягати інформаційної переваги, швидше виявляти загрози, зменшувати навантаження на особовий склад та зберігати життя. Для успішного впровадження ШІ необхідним є цілісний підхід, в якому враховуються такі концептуальні напрями впровадження:

1. Різноманітність напрямів і технологій. Штучний інтелект – це не одна технологія, а екосистема спеціалізованих моделей: трансформери, згорткові та графові мережі, автоенкодери, генеративні моделі тощо. Кожна з них вирішує окремий перелік завдань: від оброблення мовлення і тексту до аналізу відео з дронів та моделювання бойових сценаріїв. Розгортання такої системи потребує глибокої інженерної інтеграції;

2. Організаційна структура і команди. Упровадження ШІ неможливе без міждисциплінарних команд, до складу яких входять фахівці з машинного навчання, кіберзахисту, військові аналітики, фахівці з розвідки, програмісти вбудованих систем, юристи й аудитори. Лише комплексна взаємодія дасть змогу створити не просто технологію, а бойовий засіб, який відповідає етичним, правовим та оперативним вимогам;

3. Централізовані і децентралізовані рішення. Централізована модель (державна / відомча платформа ШІ) забезпечує стандартизацію, контроль, аудит та масштабованість, але є критично уразливою до централізованих атак. Децентралізовані edge-рішення забезпечують оперативність, стійкість у бойових умовах та автономність, однак ускладнюють контроль, логування та юридичне забезпечення дій системи. Гібридний підхід, що поєднує обидва підходи, є найбільш практичним і гнучким для реалізації ідеї державної / відомчої платформи;

4. Правові і безпекові межі. Штучний інтелект у військовому секторі є також джерелом юридичних викликів: хто несе відповідальність за його помилки, як забезпечити прозорість рішень, як обмежити автономне застосування летальної сили, як узгодити використання персональних і розвідувальних даних із законодавством? Відповіді на ці запитання мають бути закріплені через національну стратегію, етичний кодекс ШІ, нормативну базу та обов'язкову сертифікацію систем (системи захисту інформації, Common Criteria тощо).

5. Інфраструктура. Інфраструктура ШІ має відповідати двом одночасним вимогам: бути масштабованою і захищеною. Це означає використання кластерів із GPU/TPU, хмарних рішень із Zero Trust-доступом, а також вбудованих пристроїв для польових умов, які здатні працювати в умовах радіоелектронної боротьби та перебоїв із живленням. Україна має шанс не просто інтегрувати ШІ у військові структури, а й стати одним із лідерів у формуванні військово-етичної, правової та інженерної культури його використання у бойових умовах. Для цього необхідно: створити державну координаційну платформу ШІ у сфері безпеки і оборони; побудувати гібридну екосистему централізованих і edge-систем; затвердити юридичні й безпекові стандарти; інвестувати у навчання і формування команд, в яких військові і технічні фахівці працюють спільно.

Сили оборони є ключовим стейкхолдером, однак ефективна державна платформа ШІ не може бути створена виключно у військовому середовищі. Залучення цивільних розробників, науковців та незалежних експертів підвищує якість ухвалених рішень. Штучний інтелект має «працювати» на оборону, але створюватися у співпраці з науковцями, цивільними технологічними компаніями та підрозділами Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, а також на підприємствах Оборонно-промислового комплексу України. Подальші наукові дослідження будуть спрямовані на вирішення зазначених питань.

Список використаної літератури:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.
2. *Korniienko V.* Organizational and legal principles of use artificial intelligence in the field of state security/ *V.Korniienko, V.Hmyria, M.Styshuk* // Честь і Закон. – 2025. – № 1(92). – С. 59–69.
3. *Tkachenko K.* The impact of artificial intelligence on the development of armed conflicts / *K.Tkachenko, S.Bielai* // Безпека держави. – 2024. – Вип. 2 (4). – С. 90–97.
4. *Пантєлєєва Н.М.* Штучний інтелект як радикальна інновація трансформаційних змін природи і характеру війн / *Н.М. Пантєлєєва* // Наука і техніка Повітряних Сил Збройних Сил України. – 2024. – № 2 (55). –С. 7–15.
5. Удосконалення військової гри за допомогою штучного інтелекту : перший крок у побудові довіри до людино-машинної команди / *В.М. Приміренко, П.Даглес, Е.Лі, Г.Седрік* // Сучасні інформаційні технології у сфері безпеки та оборони. – 2025. – № 52 (1). – С. 108–117.

6. *Гусак Ю.А.* Сучасні аспекти використання штучного інтелекту Збройними Силами України в умовах воєнного стану / *Ю.А. Гусак, С.В. Кітік, Д.В. Кандуєв* // Актуальні проблеми вітчизняної юриспруденції. – 2023. – № 2. – С. 91–95.
7. *Гуржій С.В.* Тенденції застосування технологій штучного інтелекту у військово-технічній сфері / *С.В. Гуржій* // Інформація і право. – 2024. – № 3 (50). – С. 136–146.

References:

1. Kabinet Ministriv Ukrainy (2020), «Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini», Rozporiadzhennia vid 02 hrudnia 2020 r. No. 1556, [Online], available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
2. Korniienko, V., Hmyria, V. and Styshuk, M. (2025), «Organizational and legal principles of use artificial intelligence in the field of state security», *Chest i zakon*, Vol. 1 (92), pp. 59−69.
3. Tkachenko, K. and Bielai, S. (2024), «The impact of artificial intelligence on the development of armed conflicts», *Bezpeka derzhavy*, Vol. 2 (4), pp. 90−97.
4. Pantielieieva, N.M. (2024), «Shtuchnyi intelekt yak radykalna innovatsiia transformatsiinykh zmin pryrody i kharakteru viin», *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, Vol. 2 (55), pp. 7−15.
5. Prymirenko, V.M., Dahles, P., Li, E. and Sedrik, H. (2025), «Udoskonalennia viiskovoi hry za dopomohoiu shtuchnoho intelektu: pershyi krok u pobudovi doviry do liudyno-mashynnoi komandy», *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, Vol. 52 (1), pp. 108−117.
6. Husak, Yu.A., Kitik, S.V. and Kanduiev, D.V. (2023), «Suchasni aspekty vykorystannia shtuchnoho intelektu Zbroinymy Sylamy Ukrainy v umovakh voiennoho stanu», *Aktualni problemy vitchyznianoi yurysprudentsii*, Vol. 2, pp. 91−95.
7. Hurzhii, S.V. (2024), «Tendentsii zastosuvannia tekhnolohii shtuchnoho intelektu u viiskovo-tekhnichnii sferi», *Informatsiia i pravo*, Vol. 3 (50), pp. 136−146.

Pivnenko O., Hladkov V., Bielai S., Maksym S., Dmytro P.

Justification of conceptual directions for the implementation of artificial intelligence for the needs of Ukraine's security and defense sector

Abstract. he issue of justifying conceptual directions for the implementation of artificial intelligence for the needs of Ukraine's security and defense sector has been studied. It has been established that despite the wide range of research on the development and application of artificial intelligence in the field of security and defense, the study of the conceptual aspects of its implementation for the needs of the security and defense sector has not been given sufficient attention in scientific works, which has made the chosen research direction relevant. The purpose of the article is to conduct an in-depth study of the use of artificial intelligence in the functioning of the security and defense sector and to justify the relevant conceptual directions for its implementation. To create a nationwide (departmental, interdepartmental) artificial intelligence platform, especially in the context of security and defense, the “Science – Development – Use” approach is proposed. It has been proven that this approach contributes to ensuring consistency, transparency, and efficiency at every stage, allowing for the avoidance of technocratic or isolated decisions that do not respond to real challenges. It is argued that the defense forces are a key stakeholder, but an effective state artificial intelligence platform cannot be created exclusively in a military environment. It is noted that the involvement of civilian developers, scientists, and independent experts improves the quality of decision-making. Artificial intelligence should «work» for defense, but it should be created in cooperation with scientists, civilian technology companies, and departments of the Ministry of Defense of Ukraine, the Ministry of Internal Affairs of Ukraine, the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, as well as enterprises of the defense-industrial complex of Ukraine.

Keywords: artificial intelligence; state security; security and defense sector; conceptual directions; implementation sequence; platform.

Стаття надійшла до редакції 01.06.2025.