УДК 351.86:004.8:004.056
JEL Classification: H56, H83, O33

ТИПОЛОГІЯ ЗАСТОСУВАНЬ ШТУЧНОГО ІНТЕЛЕКТУ В ОБОРОННИХ СИСТЕМАХ УКРАЇНИ: КІБЕРБЕЗПЕКОВИЙ ТА УПРАВЛІНСЬКИЙ АСПЕКТИ

СПОРИШЕВ Костянтин[1], БОНДАРЕНКО Олександр[2]
[1]Національна академія Національної гвардії України
https://orcid.org/0000-0003-4737-9698
e-mail: spor_kos@ukr.net
[2] Національна академія Національної гвардії України
https://orcid.org/0000-0003-1755-3333
e-mail: Alexanderbondarenko77@gmail.com

Стаття присвячена систематизації застосувань штучного інтелекту в оборонних системах України за критерієм поєднання кібербезпекового та управлінського вимірів. Актуальність дослідження зумовлена тим, що практика впровадження ШІ в оборонну сферу випереджає теоретичне осмислення її типологічної структури, унеможливлюючи послідовну державну політику регулювання. Метою статті є розроблення типології застосувань штучного інтелекту в оборонних системах України, що поєднує кібербезпековий та управлінський аспекти кожного класу. Використано системний підхід, метод класифікації, контент-аналіз наукових і документальних джерел. Виокремлено чотири класи застосувань ШІ – розвідувально-аналітичний, кіберзахисний, автономно-операційний та логістично-управлінський, – для кожного з яких визначено характерний кібербезпековий ризик і відповідну управлінську імплікацію. Наукова новизна полягає в тому, що, на відміну від наявних класифікацій, які розглядають кібербезпекові й управлінські аспекти застосувань ШІ окремо, запропонована типологія поєднує обидва виміри в межах кожного класу, що дає змогу узгоджено визначати як технічні заходи захисту, так і управлінські рішення для кожного типу застосувань. Практичне значення результатів полягає в можливості їх використання для розроблення диференційованої державної політики регулювання ШІ в секторі безпеки і оборони України.

Ключові слова: штучний інтелект, оборонні системи, кібербезпека, обороноздатність, державне управління, типологія, управлінські рішення, цифровізація.

https://doi.org/10.31891/mdes/2026-21-37

Стаття надійшла до редакції / Received 26.06.2026
Прийнята до друку / Accepted 30.07.2026
Опубліковано / Published 27.08.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Обороноздатність держави в умовах повномасштабної збройної агресії дедалі більшою мірою залежить від здатності системи державного управління послідовно впроваджувати технології штучного інтелекту в оборонних системах – від аналітичних платформ і систем кіберзахисту до автономних засобів ураження. Водночас практика такого впровадження в Україні та світі суттєво випереджає теоретичне осмислення її структури: рішення про застосування конкретного типу ШІ-системи ухвалюються ситуативно, без чіткого розуміння того, до якого класу застосувань вона належить, які кібербезпекові ризики притаманні саме цьому класу і яких управлінських рішень він потребує.

Інституційним втіленням цього виклику є оборонний кластер Brave1, створений у 2023 році як координаційна платформа, що об'єднує учасників сфери оборонних технологій і надає їм організаційну, інформаційну та фінансову підтримку; станом на середину 2026 року платформа об'єднує понад 1500 розробників і надала понад 570 грантів на розробки у сфері безпілотних систем, робототехніки, радіоелектронної боротьби та штучного інтелекту [21]. Практика Brave1 підтверджує загальносвітову тенденцію, згідно з якою розвідувальні та оборонні відомства дедалі більше покладаються на приватний сектор для ідентифікації, розроблення та впровадження новітніх технологій, що вимагає адаптивних механізмів взаємодії, здатних збалансувати ризики й можливості на кожному рівні технологічної готовності [19].

Проблема посилюється тим, що кібербезпековий і управлінський виміри застосувань ШІ в оборонній сфері здебільшого досліджуються окремо один від одного: технічна література зосереджується на архітектурі систем виявлення загроз, тоді як управлінська – на інституційних механізмах координації, не поєднуючи ці два виміри в межах єдиної типології. Це ускладнює формування диференційованої державної політики, яка б враховувала специфіку кожного класу застосувань одночасно в технічному й управлінському вимірах. Зазначене зумовлює потребу

розроблення типології застосувань штучного інтелекту в оборонних системах України, що поєднує кібербезпековий та управлінський аспекти кожного виокремленого класу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Впливу цифрових технологій на інформаційну безпеку в системі публічного управління присвячено дослідження М. Дурмана зі співавторами, яке на матеріалі десяти держав за 2017–2024 роки показало, що інтеграція технологій штучного інтелекту (зокрема AI-driven Threat Intelligence) забезпечує зниження кількості успішних кібератак, водночас вимагаючи від держав постійного нарощування видатків на кібербезпекову інфраструктуру [1]. Е. Щепанюк зі співавторами на основі емпіричного обстеження органів публічного управління Польщі протягом 2016–2019 років встановили, що більшість із них на початковому етапі не мала документованих процедур системи управління інформаційною безпекою (ISMS), відповідної стандарту ISO/IEC 27001, і обґрунтували доцільність застосування циклу Демінга (PDCA) як моделі безперервного вдосконалення такої системи [2, с. 3, 7]. С. Онопрієнко дослідила функції забезпечення інформаційної безпеки публічного управління України в умовах повномасштабної збройної агресії, наголосивши на ролі інституційних механізмів і національних центрів моніторингу загроз [3]. П. Хенмен на матеріалі застосувань ШІ в публічних послугах виокремив чотири управлінські виклики їх упровадження – точність і недискримінаційність рішень, законність і адміністративну справедливість, підзвітність і пояснюваність, а також владний контроль і комплаєнс, – прямо корелюючи з управлінськими імплікаціями, визначеними в цій статті для кожного класу типології [4].

Прикладний аналіз А. Гриндея за напрямами розвідки, логістики та автономних бойових систем підтверджує, що потенціал ШІ для посилення обороноздатності реалізується лише за умови паралельного розв'язання технічних, правових і гуманітарних питань [5]. У праці О. Трофименко зі співавторами військове застосування ШІ проаналізовано саме в поєднанні двох вимірів – кібербезпекового убезпечення систем і автоматизації управлінських рішень – [6, с. 167–169], що методологічно суголосно предмету цієї статті. А. Свінцицький детально реконструював інституційну архітектуру органів кібербезпеки України [7, с. 288–296]. Ці праці зосереджені або на технічному, або на управлінському вимірі застосувань ШІ, або на їх загальній характеристиці без класифікації за типами; жодна з них не пропонує типології, яка б системно поєднувала кібербезпековий і управлінський аспекти в межах кожного окремого класу застосувань.

Показово, що навіть дослідження, найближчі за предметом до цієї статті, самі фіксують цю прогалину опосередковано. Так, підсумовуючи огляд наявних підходів до інформаційної безпеки в публічному управлінні, М. Дурман зі співавторами зазначають: «спільним для різних поглядів на інформаційну безпеку в публічному управлінні є проблема інтеграції різних технологій з адміністративними процесами та ефективного захисту» [1, с. 402] – тобто йдеться про інтеграцію технологій з процесами загалом, без розмежування того, яка саме технологія потребує переважно технічного, а яка – переважно управлінського реагування. Автори також прямо протиставляють свій внесок працям, зосередженим на «виявленні вразливостей і механізмах аудиту» [1, с. 402], тоді як власний предмет дослідження визначають через «взаємодію новітніх технологій, таких як ШІ, хмарні сервіси та законодавчі механізми» [1, с. 402] – формулювання, яке також не передбачає систематичного поєднання саме кібербезпекового й управлінського вимірів у межах окремих класів застосувань, а розглядає технології, хмарні сервіси й законодавство як паралельні, а не структуровані за єдиним критерієм предмети аналізу. Це підтверджує, що навіть у найбільш дотичній літературі кібербезпековий і управлінський аспекти лишаються методологічно розведеними, а не поєднаними в межах єдиної типології.

Невирішеною частиною проблеми залишається відсутність такої двовимірної типології – що й визначило мету цієї статті.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті – розробити типологію застосувань штучного інтелекту в оборонних системах України, що поєднує кібербезпековий та управлінський аспекти кожного класу.

Завдання дослідження.

1. Визначити критерій виокремлення класів застосувань штучного інтелекту в оборонних системах.

2. Охарактеризувати кібербезпековий вимір кожного виокремленого класу застосувань.

3. Визначити управлінську імплікацію, притаманну кожному класу застосувань.

4. Встановити закономірність співвідношення кібербезпекового та управлінського вимірів між класами.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для досягнення мети застосовано системний підхід – для розгляду застосувань ШІ як цілісної, а не розрізненої за вимірами сукупності; метод класифікації – для виокремлення класів за спільним критерієм функціонального призначення; контент-аналіз наукових і документальних джерел – для визначення кібербезпекового та управлінського змісту кожного класу.

Критерій та структура типології. Для формування типології проаналізовано задокументовані практики застосування ШІ, представлені в чотирьох групах джерел:

- по-перше, статистику видатків на кібербезпеку та перелік резонансних інцидентів у десяти державах за 2017–2024 роки [1];
- по-друге, прикладний аналіз розвідувальних, логістичних та автономних бойових систем на матеріалі оборонної сфери [5] і військової сфери крізь призму кібербезпеки та автоматизації рішень [6];
- по-третє, реконструйовану інституційну архітектуру органів кібербезпеки України [7];
- по-четверте, окремі задокументовані інциденти – кампанію UAC-0219/WRECKSTEEL [8] та першу оприлюднену кібершпигунську кампанію, оркестровану ШІ [9].

Зіставлення цих практик між собою показало, що вони не групуються послідовно за типом технології (машинне навчання, комп'ютерний зір тощо) – та сама технологія машинного навчання застосовується і в аналітичних платформах, і в автономних системах ураження, – натомість вони послідовно розрізняються за тим, НА ЯКОМУ ЕТАПІ управлінського й безпекового циклу відбувається застосування ШІ: збір і аналіз інформації до ухвалення рішення (клас 1), захист інфраструктури під час штатного функціонування (клас 2), виконання дій з мінімальною участю людини (клас 3), або забезпечення ресурсної основи для перших трьох (клас 4).

Саме тому критерієм класифікації обрано функціональне призначення застосування, а не тип базової технології: перший критерій системно пояснює, чому кожен клас має свою специфічну пропорцію кібербезпекового й управлінського вимірів, тоді як групування за технологією цієї закономірності не виявляє. На основі зазначеного виокремлено чотири класи, кожен з яких послідовно характеризується через два виміри: кібербезпековий (характерний ризик або захисна функція) та управлінський (відповідне управлінське рішення чи інституційна імплікація). Узагальнено типологію представлено на рис. 1.

Клас 1. Розвідувально-аналітичний. Охоплює застосування ШІ для аналізу розвідувальних даних і прогнозування загроз, зокрема через технології AI-driven Threat Intelligence, які забезпечують безперервний моніторинг і аналіз кіберзагроз у реальному часі [1]. Кібербезпековий вимір цього класу полягає у виявленні аномалій способом, який перевищує можливості ручного аналізу; управлінський – у формуванні системи підтримки прийняття рішень для командування, що потребує розмежування функцій людини-оператора та автоматизованої системи; профільний аналітичний звіт Науково-технічної організації НАТО щодо когнітивного протиборства зараховує технологічно підсилені впливи на людське сприйняття до самостійного предмета розвідувально-аналітичної роботи [18]. Прикладом практичної реалізації цього класу є системи типу SIEM з інтегрованим ШІ-аналізом подій, які на матеріалі десяти держав за 2017–2024 роки продемонстрували скорочення часу виявлення кіберзагроз [1], а також платформи прогнозування атак на критичну інфраструктуру – енергетичні мережі й транспортні системи, – що застосовують машинне навчання для завчасного визначення вразливостей. Показовою є глобальна динаміка: сукупні видатки на кібербезпеку зросли з 34 млрд дол. США 2017 року до прогнозованих 87 млрд дол. 2024 року, причому найбільший стрибок припав саме на 2020–2022 роки – період пандемійного переходу на дистанційну роботу та ескалації збройної агресії проти України, що прямо підтверджує кореляцію між масштабом безпекових викликів і темпами впровадження аналітичних ШІ-рішень [1]. Управлінська імплікація цього зв'язку полягає в тому, що бюджетування розвідувально-аналітичного класу застосувань не може плануватися на довгостроковій, статичній основі – воно потребує гнучких, оперативно коригованих процедур фінансування, здатних реагувати на різкі зміни безпекового середовища.

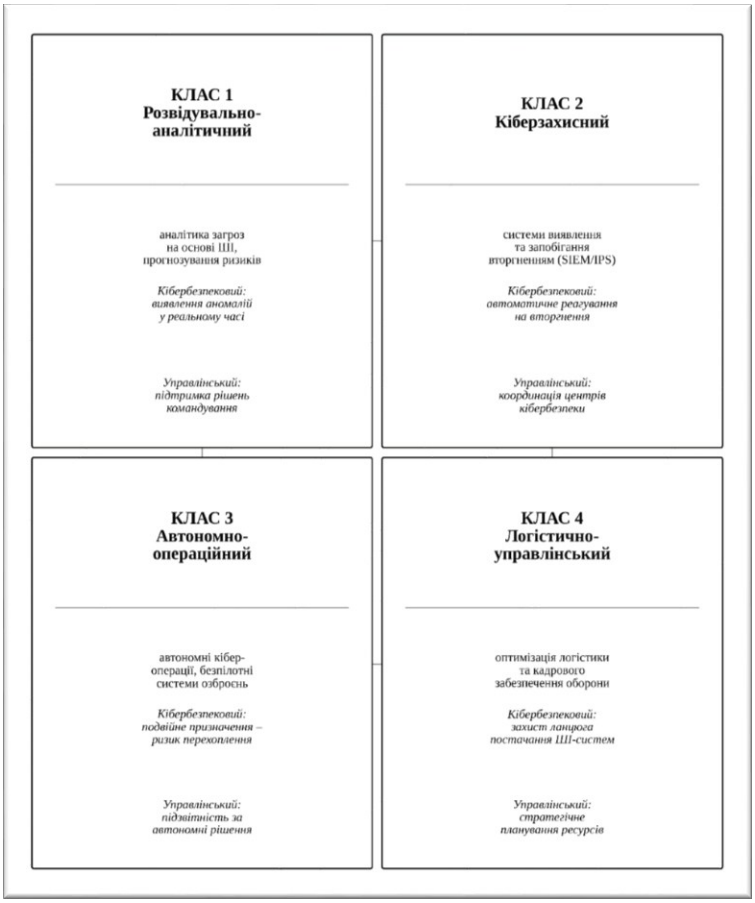

Рис. 1. Типологія застосувань штучного інтелекту в оборонних системах України
Джерело: розроблено автором

Клас 2. Кіберзахисний. Охоплює системи класу SIEM (Security Information and Event Management) та IDS/IPS (Intrusion Detection System/Intrusion Prevention System) на основі ШІ, призначені для захисту критичної інфраструктури, включно з енергетичною та оборонною [1]. Українська практика підтверджує актуальність цього класу: кампанія кібершпигунської групи UAC-0219 з використанням шкідливого інструменту WRECKSTEEL, спрямована проти органів державної влади й об'єктів критичної інфраструктури, ілюструє необхідність автоматизованого реагування на вторгнення [8]. Управлінський вимір полягає в координації діяльності спеціалізованих центрів кібербезпеки – зокрема Національного координаційного центру кібербезпеки та CERT-UA, інституційна архітектура яких склалася протягом 2007–2016 років [7, с. 288–296], на засадах, закладених чинною Стратегією кібербезпеки України [17]. Показовим прикладом застосування цього класу є задокументована серія DDoS-атак на енергетичний сектор та органи публічного управління України після 24 лютого 2022 року, спрямована на дестабілізацію критичної інфраструктури в умовах воєнного стану [1], а також системи класу IDS/IPS, що використовуються для протидії атакам на державні портали електронних послуг за зразком «Дії». Міжнародний досвід підтверджує універсальність цього класу: у 2022–2024 роках задокументовано резонансні кібератаки на органи публічного управління Коста-Рики, Великої Британії, Німеччини, Австралії, Японії та Франції, спричинені здебільшого програмами-вимагачами й розподіленими атаками на відмову в обслуговуванні [1]. Людський фактор залишається наскрізною вразливістю навіть за наявності технічних засобів захисту: за узагальненими даними, 88 % кіберінцидентів у державних органах пов'язані саме з людськими помилками в управлінні інформацією, що визначає управлінську імплікацію цього класу – впровадження ШІ-рішень має супроводжуватися не лише технічною інтеграцією, а й систематичним навчанням персоналу, оскільки жодна автоматизована система виявлення вторгнень не компенсує людської неуважності на етапі первинного доступу [1].

Клас 3. Автономно-операційний. Охоплює автономні кібероперації та безпілотні системи озброєнь, здатні виконувати тактичні завдання без безпосередньої участі людини-оператора на кожному етапі. Задокументований випадок, коли роль людини-оператора звузилася до

затвердження стратегічних кроків, а решту тактичного циклу кібероперації виконала автономна агентна система [9], ілюструє кібербезпековий ризик цього класу: подвійне призначення технології робить її вразливою до перехоплення й використання супротивником. Управлінський вимір полягає в забезпеченні підзвітності за рішення, ухвалені автономними системами, – питання, що перебуває в порядку денному профільної Групи урядових експертів при ООН, зосередженої на летальних автономних системах озброєнь [10] а її довгострокову динаміку простежено П. Шарре на прикладі багаторічної еволюції автономних озброєнь [11]. Прикладом цього класу є безпілотні авіаційні комплекси з елементами автономного наведення та розпізнавання цілей, а також задокументована практика автономного виконання етапів кібероперації – розвідки, експлуатації вразливостей і ексфільтрації даних – без постійного втручання оператора на кожному кроці [9]. Управлінська імплікація цього класу є найгострішою серед усіх чотирьох: якщо для класів 1–2 підзвітність зводиться до аудиту технічних логів, то для автономно-операційного класу йдеться про принципову межу делегування права ухвалення рішень від людини до системи, що на міжнародному рівні залишається предметом невирішеної дискусії навіть у межах профільної Групи урядових експертів ООН [10], а отже вимагає від національної системи державного управління випереджального, а не запозиченого регуляторного рішення.

Клас 4. Логістично-управлінський. Охоплює застосування ШІ для оптимізації логістики, розподілу ресурсів і кадрового забезпечення оборонного сектору. На відміну від перших трьох класів, кібербезпековий ризик тут полягає не в прямому кібербойовому застосуванні, а в уразливості ланцюга постачання самих ШІ-систем – компрометації даних чи моделей, на основі яких ухвалюються логістичні рішення [12]. Управлінський вимір є в цьому класі домінівним: ідеться про стратегічне планування розподілу ресурсів, що потребує інтеграції ШІ-рекомендацій у чинні процедури прийняття управлінських рішень, а не про операційне кіберреагування. Прикладом застосувань цього класу є системи підтримки планування постачання озброєння та боєприпасів, а також платформи прогнозування кадрових потреб оборонного сектору на основі аналізу історичних даних про втрати й ротацію особового складу. Управлінська специфіка цього класу підтверджується й тим, що, на відміну від класів 1–3, де провідну роль відіграють підрозділи технічного й безпекового профілю, тут ключовим суб'єктом ухвалення рішень залишаються органи стратегічного планування та фінансово-економічні підрозділи оборонного відомства, для яких ШІ-рекомендація є одним із джерел управлінської інформації, а не автономною дією, що потребує окремого контуру підзвітності.

Наскрізний інституційний вимір. Окрім специфічного для кожного класу співвідношення кібербезпекового й управлінського вимірів, усі чотири класи об'єднує наскрізна залежність від моделі публічно-приватної взаємодії. методологічно це узгоджується з висновком С. Бєлая зі співавторами про доцільність поєднання теоретичного і прикладного рівнів аналізу при управлінні національною безпекою [20] – методологія, застосовна до кожного з виокремлених класів, оскільки жоден із них не реалізується виключно засобами державного сектору: розвідувально-аналітичний і кіберзахисний класи спираються на технологічну експертизу приватних розробників у межах Brave1 [21], автономно-операційний клас – на партнерство з виробниками безпілотних систем, а логістично-управлінський – на цифрові платформи приватних постачальників. Це узгоджується з висновком Д. ван Пейвельде та П. Оулінга про те, що успішність упровадження новітніх технологій в оборонному секторі визначається не лише технологічною готовністю рішення, а й гнучкістю механізмів ранньої та сталої взаємодії між державними замовниками й приватними розробниками [19]. Наскрізний характер цієї залежності означає, що диференційована політика регулювання, обґрунтована в підрозділі щодо окремих класів, має доповнюватися єдиними, спільними для всіх класів вимогами до публічно-приватної взаємодії – прозорості конкурсного відбору, захисту прав інтелектуальної власності розробників і чіткого розмежування відповідальності між державним замовником і приватним виконавцем.

Порівняння запропонованої типології з наявними класифікаціями показує її відмінність від підходів, які структурують застосування ШІ за технологічним принципом (машинне навчання, комп'ютерний зір, обробка природної мови) [2] або за рівнем зрілості впровадження [4]: на відміну від них, критерій функціонального призначення, покладений в основу цієї типології, дає змогу прогнозувати не лише те, ЯКА технологія застосовується, а й ЯКИЙ управлінський орган і за якою процедурою має ухвалювати рішення щодо неї, що є прямим практичним виходом дослідження для формування організаційної структури профільних підрозділів у секторі безпеки і оборони.

Узагальнення типології. Порівняння чотирьох класів засвідчує закономірність: питома вага кібербезпекового виміру послідовно знижується від першого до четвертого класу (від переважно

технічного виявлення аномалій до переважно управлінського планування), тоді як питома вага управлінського виміру, навпаки, зростає. Це означає, що диференційована державна політика регулювання ШІ в оборонній сфері не може спиратися на єдиний універсальний підхід: для класів 1–2 пріоритетними є технічні стандарти й акредитація систем виявлення загроз, тоді як для класів 3–4 – розроблення процедур підзвітності та інтеграції ШІ-рекомендацій у прийняття стратегічних рішень. Регуляторним орієнтиром для перших двох класів можуть слугувати підходи, закладені в Регламенті (ЄС) 2024/1689 про штучний інтелект та Директиві NIS2 [13; 14], тоді як для класів 3–4 – радше в документах на кшталт Концепції розвитку штучного інтелекту в Україні [15] та Закону України «Про національну безпеку України» [16], що визначають інституційні рамки прийняття рішень.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті розроблено типологію застосувань штучного інтелекту в оборонних системах України, що поєднує кібербезпековий та управлінський аспекти кожного класу. Виокремлено чотири класи – розвідувально-аналітичний, кіберзахисний, автономно-операційний та логістично-управлінський, – для кожного з яких визначено характерний кібербезпековий ризик і відповідне управлінське рішення. Встановлено закономірність: питома вага кібербезпекового виміру послідовно знижується від першого до четвертого класу, тоді як управлінського – зростає, що обґрунтовує потребу диференційованої, а не універсальної державної політики регулювання ШІ в оборонній сфері.

Власне новим результатом є поєднання кібербезпекового та управлінського вимірів у межах єдиної чотирикласової типології та встановлена закономірність їх обернено пропорційної питомої ваги; характеристика окремих технологій (SIEM, AI-driven Threat Intelligence, автономні системи) є узагальненням наявних у літературі та задокументованих положень, використаним як емпірична основа для побудови типології.

Перспективи подальших досліджень пов'язані передусім з операціоналізацією запропонованої типології через систему кількісних індикаторів для кожного класу: для розвідувально-аналітичного та кіберзахисного класів такими індикаторами можуть слугувати час виявлення й реагування на інцидент, частка хибнопозитивних спрацювань та рівень автоматизації циклу виявлення–реагування, тоді як для автономно-операційного й логістично-управлінського класів – частка рішень, ухвалених без безпосередньої участі людини-оператора, та частка бюджету оборонних закупівель, розподілена на основі ШІ-рекомендацій. Побудова такої системи індикаторів дасть змогу емпірично перевірити встановлену в статті закономірність обернено пропорційного співвідношення кібербезпекового й управлінського вимірів між класами, а не лише постулювати її якісно.

Другим напрямом є розроблення на основі запропонованої типології диференційованого механізму державного регулювання застосувань штучного інтелекту в секторі безпеки і оборони України, який, на відміну від уніфікованих підходів, встановлював би окремі регуляторні вимоги для кожного класу – технічну акредитацію та стандарти взаємосумісності для розвідувально-аналітичного й кіберзахисного класів, процедури підзвітності та людського контролю для автономно-операційного класу, вимоги до аудиту й прозорості алгоритмів прийняття рішень для логістично-управлінського класу.

Третім, наскрізним напрямом, що випливає з виявленої залежності всіх класів від моделі публічно-приватної взаємодії, є дослідження оптимальних форм такої взаємодії окремо для кожного класу – від відкритих конкурсних процедур для логістично-управлінського класу до обмежених, попередньо перевірених партнерств для класів, пов'язаних з автономним застосуванням сили.

ЛІТЕРАТУРА:

1. Durman M., Durman O., Drozhzhyn D., Krylova I., Gavrylechko Y. Influence of Digital Technologies on Information Security in the Public Administration System. Journal of Theoretical and Applied Information Technology. 2025. Vol. 103, No. 2. P. 400–422. URL: https://jatit.org/volumes/Vol103No2/3Vol103No2.pdf

2. Szczepaniuk E.K., Szczepaniuk H., Rokicki T., Klepacki B. Information Security Assessment in Public Administration. Computers and Security. 2020. Vol. 90. Art. 101709. DOI: https://doi.org/10.1016/j.cose.2019.101709

3. Onopriienko S. Functions of Ensuring Information Security of Public Administration in Ukraine in the Face of Full-Scale Armed Aggression of the Russian Federation. Visnyk Taras Shevchenko National University of Kyiv. Military-Special Sciences. 2022. P. 95–98. https://doi.org/10.17721/1728-2217.2022.50.95-98

4. Henman P. Improving Public Services Using Artificial Intelligence: Possibilities, Pitfalls, Governance. Asia Pacific Journal of Public Administration. 2020. Vol. 42, No. 4. P. 209–221. https://doi.org/10.1080/23276665.2020.1816188

5. Гриндей А.О. Використання штучного інтелекту в оборонній сфері. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. 2024. Т. 35(74), № 6. С. 120–123. https://doi.org/10.32782/TNU-2663-6468/2024.6/21

6. Трофименко О., Логінова Н., Соколов А., Чикунов П., Ахмаметьєва Г. Штучний інтелект у військовій сфері. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. № 1(25). С. 161–176. DOI: 10.28925/2663-4023.2024.25.161176.

7. Svintsytskyi A.V. The system of cybersecurity bodies in Ukraine. Revista Científica General José María Córdova. 2022. Vol. 20, No. 38. P. 287–305. DOI: 10.21830/19006586.903.

8. CERT-UA, Державна служба спеціального зв'язку та захисту інформації України. UAC-0219: кібершпигунство з використанням PowerShell-стілеру WRECKSTEEL (CERT-UA#14283). 2025. URL: https://cert.gov.ua/article/6282902 (дата звернення: 13.08.2026).

9. Disrupting the first reported AI-orchestrated cyber espionage campaign. Anthropic. 2025. URL: https://www.anthropic.com/news/disrupting-AI-espionage (дата звернення: 13.08.2026).

10. Convention on Certain Conventional Weapons – Group of Governmental Experts on Lethal Autonomous Weapons Systems. United Nations Office for Disarmament Affairs. URL: https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2026 (дата звернення: 13.08.2026).

11. Scharre P. Army of None: Autonomous Weapons and the Future of War. New York: W.W. Norton & Company, 2018. 436 p. ISBN 978-0-393-35658-8.

12. MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems). MITRE Corporation. 2025. URL: https://atlas.mitre.org/ (дата звернення: 13.08.2026).

13. 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. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 13.08.2026).

14. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

15. 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

16. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19

17. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

18. NATO Chief Scientist Research Report on Cognitive Warfare. NATO Science and Technology Organization. 2025. URL: https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-final.pdf (дата звернення: 13.08.2026).

19. Van Puyvelde D., Oling P. Public-private collaboration and the digital transformation of intelligence. Intelligence and National Security. 2025. Vol. 40, No. 6. P. 1015–1030. DOI: 10.1080/02684527.2025.2565950.

20. Bielai S., Antonova L., Hololobov S., Yevtushenko I., Sporyshev K. The Impact of a Practice-Oriented Paradigm on Public Administration and National Security. International Journal of Sustainable Development and Planning. 2024. Vol. 19, No. 1. P. 291–300. DOI: 10.18280/ijsdp.190126.

21. Brave1. Проєкти. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/projects/technologies/brave1 (дата звернення: 13.08.2026).

REFERENCES:

1. Durman, M., Durman, O., Drozhzhyn, D., Krylova, I. and Gavrylechko, Y. (2025), "Influence of Digital Technologies on Information Security in the Public Administration System", Journal of Theoretical and Applied Information Technology, Vol. 103, No. 2, pp. 400-422, available at: https://jatit.org/volumes/Vol103No2/3Vol103No2.pdf (accessed 13 August 2026).

2. Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T. and Klepacki, B. (2020), "Information Security Assessment in Public Administration", Computers and Security, Vol. 90, Art. 101709, DOI: 10.1016/j.cose.2019.101709.

3. Onopriienko, S. (2022), "Functions of Ensuring Information Security of Public Administration in Ukraine in the Face of Full-Scale Armed Aggression of the Russian Federation", Visnyk Taras Shevchenko National University of Kyiv. Military-Special Sciences, pp. 95-98, DOI: 10.17721/1728-2217.2022.50.95-98

4. Henman, P. (2020), "Improving Public Services Using Artificial Intelligence: Possibilities, Pitfalls, Governance", Asia Pacific Journal of Public Administration, Vol. 42, No. 4, pp. 209-221, DOI: 10.1080/23276665.2020.1816188.

5. Hryndei, A.O. (2024), "Vykorystannia shtuchnoho intelektu v oboronnii sferi" [Use of artificial intelligence in the defense sphere], Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia, Vol. 35(74), No. 6, pp. 120-123, DOI: 10.32782/TNU-2663-6468/2024.6/21. [in Ukrainian].

6. Trofymenko, O., Loginova, N., Sokolov, A., Chykunov, P. and Akhmametieva, H. (2024), "Shtuchnyi intelekt u viiskovii sferi" [Artificial intelligence in the military sphere], Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika", No. 1(25), pp. 161-176, DOI: 10.28925/2663-4023.2024.25.161176. [in Ukrainian].

7. Svintsytskyi, A.V. (2022), "The system of cybersecurity bodies in Ukraine", Revista Científica General José María Córdova, Vol. 20, No. 38, pp. 287-305, DOI: 10.21830/19006586.903.

8. CERT-UA, State Service of Special Communications and Information Protection of Ukraine (2025), "UAC-0219: cyber espionage using the WRECKSTEEL PowerShell stealer (CERT-UA#14283)", available at: https://cert.gov.ua/article/6282902 (accessed 13 August 2026). [in Ukrainian].

9. Anthropic (2025), "Disrupting the first reported AI-orchestrated cyber espionage campaign", available at: https://www.anthropic.com/news/disrupting-AI-espionage (accessed 13 August 2026).

10. United Nations Office for Disarmament Affairs, "Convention on Certain Conventional Weapons – Group of Governmental Experts on Lethal Autonomous Weapons Systems", available at: https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2026 (accessed 13 August 2026).

11. Scharre, P. (2018), Army of None: Autonomous Weapons and the Future of War, W.W. Norton & Company, New York, 436 p., ISBN 978-0-393-35658-8.

12. MITRE Corporation (2025), "MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)", available at: https://atlas.mitre.org/ (accessed 13 August 2026).

13. Official Journal of the European Union (2024), "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)", available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed 13 August 2026).

14. Official Journal of the European Union (2022), "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)", available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed 13 August 2026).

15. Cabinet of Ministers of Ukraine (2020), "Order No. 1556-r of 02.12.2020 on the Approval of the Concept for the Development of Artificial Intelligence in Ukraine", available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80 (accessed 13 August 2026). [in Ukrainian].

16. Verkhovna Rada of Ukraine (2018), "Law of Ukraine No. 2469-VIII of 21.06.2018 'On National Security of Ukraine'", available at: https://zakon.rada.gov.ua/laws/show/2469-19 (accessed 13 August 2026). [in Ukrainian].

17. President of Ukraine (2021), "Decree No. 447/2021 of 26.08.2021 'On the Cybersecurity Strategy of Ukraine'", available at: https://zakon.rada.gov.ua/laws/show/447/2021 (accessed 13 August 2026). [in Ukrainian].

18. NATO Science and Technology Organization (2025), "NATO Chief Scientist Research Report on Cognitive Warfare", available at: https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-final.pdf (accessed 13 August 2026).

19. Van Puyvelde, D. and Oling, P. (2025), "Public-private collaboration and the digital transformation of intelligence", Intelligence and National Security, Vol. 40, No. 6, pp. 1015-1030, DOI: 10.1080/02684527.2025.2565950.

20. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I. and Sporyshev, K. (2024), "The Impact of a Practice-Oriented Paradigm on Public Administration and National Security", International Journal of Sustainable Development and Planning, Vol. 19, No. 1, pp. 291-300, DOI: 10.18280/ijsdp.190126.

21. Brave1 (2026), "Proiekty" [Projects], Ministry of Digital Transformation of Ukraine, available at: https://thedigital.gov.ua/projects/technologies/brave1 (accessed 13 August 2026). [in Ukrainian].

TYPOLOGY OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN UKRAINE'S DEFENSE SYSTEMS: CYBERSECURITY AND MANAGERIAL ASPECTS

SPORYSHEV Kostyantyn, BONDARENKO Oleksandr
National Academy of the National Guard of Ukraine

The article is devoted to systematizing artificial intelligence applications in Ukraine's defense systems by the criterion of combining cybersecurity and managerial dimensions. The relevance of the study stems from the fact that the practice of AI implementation in the defense sphere outpaces the theoretical understanding of its typological structure, which precludes a coherent state regulatory policy. The article aims to develop a typology of artificial intelligence applications in Ukraine's defense systems that combines the cybersecurity and managerial aspects of each class. The study employs the systems approach, the classification method, and content analysis of scholarly and documentary sources. Four

classes of AI applications are identified – intelligence-analytical, cyber-defense, autonomous-operational, and logistics-managerial – for each of which a characteristic cybersecurity risk and a corresponding managerial implication are determined. The novelty consists in the fact that, unlike existing classifications that treat the cybersecurity and managerial aspects of AI applications separately, the proposed typology combines both dimensions within each class, enabling the coherent determination of both technical protective measures and managerial decisions for each application type. The practical significance lies in the applicability of the results to developing a differentiated state policy for regulating AI in Ukraine's security and defense sector.

Key words: artificial intelligence, defense systems, cybersecurity, defense capability, public administration, typology, managerial decisions, digitalization.