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

ОБОРОНОЗДАТНІСТЬ ДЕРЖАВИ ЯК ОБ'ЄКТ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ СТРІМКОГО РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

НЕКРЯЧ Анастасія[1], ДАБІЖА Віра[2]
[1] ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0000-0001-5058-4145
e-mail: anastasian1947@gmail.com
[2] ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0000-0002-7000-4635
e-mail: verynchik@ukr.net

Стаття присвячена концептуалізації обороноздатності держави як самостійного об'єкта публічного управління в умовах стрімкого розвитку штучного інтелекту (далі – ШІ). Актуальність дослідження зумовлена тим, що покоління великих генеративних моделей змінюються швидше, ніж законодавці й урядовці встигають на це реагувати, а поняття «обороноздатність держави», «оборона» та «національна безпека» в науковій літературі здебільшого вживаються як синоніми, що ускладнює формування чіткого предмета публічного управління в цій сфері та розмежування повноважень між суб'єктами сектору безпеки й оборони. Метою статті є концептуалізація обороноздатності держави як об'єкта публічного управління та визначення її співвідношення із суміжними категоріями в умовах поширення ШІ-технологій. Використано системний підхід, порівняльний метод, контент-аналіз наукових і нормативних джерел. Систематизовано наукові підходи до трактування обороноздатності, оборони та національної безпеки. Обґрунтовано критерії їх розмежування; визначено дуальну роль штучного інтелекту – як інструмента підвищення обороноздатності та як джерела нових асиметричних загроз. Охарактеризовано управлінські імплікації темпоральної асиметрії між циклом оновлення ШІ-технологій і циклом нормотворення. Зіставлено запропоновану концептуалізацію з альтернативними науковими позиціями. Наукова новизна полягає в обґрунтуванні обороноздатності держави як самостійного, відмінного від оборони й національної безпеки, об'єкта публічного управління, предметна межа якого визначається сукупністю керованих (а не лише природних чи безумовних) чинників спроможності держави. Практичне значення результатів полягає в можливості їх використання для вдосконалення програмних документів у сфері оборонної політики та цифрової трансформації сектору безпеки і оборони України.

Ключові слова: обороноздатність держави, державне управління, штучний інтелект, національна безпека, оборона, оборонні системи, кібербезпека, публічна влада, державне регулювання, цифровізація.

https://doi.org/10.31891/mdes/2026-21-41

Стаття надійшла до редакції / Received 01.07.2026
Прийнята до друку / Accepted 05.08.2026
Опубліковано / Published 27.08.2026

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

Повномасштабна збройна агресія проти України перетворила обороноздатність держави з переважно військово-технічної категорії на предмет системного публічного управління, що охоплює цифровізацію оборонного сектору, координацію оборонних інновацій та інтеграцію технологій штучного інтелекту в управлінські й бойові процеси. Формування оборонного кластеру Brave1, створення програми підтримки військових стартапів K4 Startup Studio Міністерства оборони України, впровадження системи ситуаційної обізнаності на кшталт Delta й Griselda – усе це свідчить, що інтеграція ШІ в оборонну сферу вже є не просто перспективною темою, а поточною управлінською практикою, яка випереджає теоретичне осмислення відповідного об'єкта публічного управління.

Водночас швидкість, з якою змінюються покоління великих генеративних моделей і автономних систем на їх основі, структурно випереджає швидкість класичного управлінського циклу «виявлення проблеми – нормування – впровадження»: законодавці й урядовці регулярно приймають рішення щодо технологій, які застарівають ще до набрання цими рішеннями чинності. Ця темпоральна асиметрія – не другорядна технічна деталь, а системна характеристика, яка має бути врахована в самій архітектурі управління обороноздатністю, інакше механізми управління структурно приречені на постійне відставання від об'єкта, яким вони покликані керувати.

Проблема посилюється термінологічною невизначеністю: поняття «обороноздатність держави», «оборона» та «національна безпека» в науковій літературі та управлінській практиці здебільшого вживаються як синоніми або через неявне включення одного в інше, без чіткого визначення предметних меж кожного. Це ускладнює формування єдиного об'єкта публічного управління у сфері оборони, розмежування повноважень між суб'єктами сектору безпеки й оборони – Міністерством оборони, Генеральним штабом, розвідувальними органами, суб'єктами

оборонно-промислового комплексу – та вироблення послідовної державної політики впровадження ШІ-технологій. Без чіткого розмежування ризик полягає в дублюванні функцій одних суб'єктів і появі управлінських прогалин там, де жоден суб'єкт не вважає конкретне питання (наприклад, кібербезпеку ШІ-систем подвійного призначення) власною зоною відповідальності.

Додаткового виміру проблемі надає дуальна природа самих технологій ШІ: ті самі можливості, що посилюють обороноздатність держави (аналіз розвідданих, автоматизація логістики, кіберзахист), в руках супротивника стають інструментом асиметричних загроз – автономних кібератак, дипфейків, генеративної дезінформації. Управлінське реагування на цю дуальність неможливе без попереднього визначення того, яким саме є об'єкт управління – обороноздатність, оборона чи національна безпека в цілому, – оскільки кожна з цих категорій передбачає різних суб'єктів відповідальності та різний інструментарій державного регулювання. Зазначене зумовлює потребу теоретико-методологічної концептуалізації обороноздатності держави саме як об'єкта публічного управління, відмінного від суміжних категорій, з урахуванням технологічної детермінанти, пов'язаної з поширенням штучного інтелекту.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Категорійний апарат науки державного управління національною безпекою як цілісною предметною сферою розроблено Г. Ситником, який визначив національну безпеку через систему категорій, функцій та організаційно-правових засад [1]. В. Ліпкан системно виклав категорійно-понятійний апарат націобезпекознавства (розділ 1, підрозділ 4) [2], що й сьогодні залишається методологічною рамкою для визначення цільової рамки управління безпековими підсистемами. В. Горбулін і В. Бадрак на матеріалі повномасштабної війни довели визначальну роль технологій у трансформації безпекового середовища, актуалізувавши потребу випереджальної інституційної відповіді [3]. Ці праці закладають загальнотеоретичну рамку національної безпеки, проте жодна з них не виокремлює обороноздатність як самостійний об'єкт управління, відмінний від національної безпеки в цілому.

Безпосередньо застосуванню ШІ в оборонній сфері присвячено праці А. Гриндея, який на основі аналізу розвідувальних, логістичних та автономних бойових систем показав, що впровадження ШІ відкриває нові можливості для посилення обороноздатності держав, водночас вимагаючи комплексного врахування технічних, правових і гуманітарних факторів [10, с. 120]. О. Трофименко зі співавторами дослідили застосування ШІ у військовій сфері крізь призму кібербезпеки й автоматизації прийняття рішень [11, с. 167–169]. Обидві праці, однак, розглядають ШІ переважно в технічній і військово-прикладній площині, не порушуючи питання про статус обороноздатності як категорії публічного управління.

Дуальна природа технологій штучного інтелекту у безпековому вимірі розкрита в наших попередніх дослідженнях: показано, що цифровізація публічного управління й масштабне впровадження ШІ-систем формують принципово нові виклики інформаційній безпеці держави, водночас розширюючи спроможності сервісної держави, а еволюція регуляторної бази ЄС – від Стратегії кібербезпеки 2013 року до Директиви NIS2 і Регламенту EU AI Act – ілюструє інституційну відповідь на цю дуальність [4]. Задокументована кампанія кібершпигунства, оркестрована штучним інтелектом, у якій до 80–90 % тактичних операцій виконувалися автономно [12], та структурована база знань MITRE ATLAS, що каталогізує тактики зловмисного використання ШІ проти ШІ-систем [13], емпірично підтверджують перехід технологічних загроз у режим автономного функціонування. Українська практика підтверджує цю тенденцію на національному рівні: CERT-UA задокументувала кампанію кібершпигунської групи UAC-0219 із застосуванням шкідливого інструменту WRECKSTEEL, імовірно створеного з використанням ШІ, спрямовану проти органів державної влади й об'єктів критичної інфраструктури, зокрема оборонного та телекомунікаційного профілю [14].

П. Шарре на матеріалі десятиліть розвитку автономних озброєнь показав, що делегування рішень автономним системам порушує етико-правові питання контрольованості, які набувають особливої гостроти для сектору оборони [15], а міжнародний рівень регулювання цієї проблеми представлений Групою урядових експертів ООН з летальних автономних систем озброєнь [16]. Дослідницький звіт Головного науковця НАТО з питань когнітивного протиборства концептуалізує технологічно підсилені впливи на людське сприйняття як самостійний клас загроз обороноздатності, що не зводиться до суто технічного чи суто інформаційного виміру [17].

У ширшому контексті публічного управління впровадженням ШІ О. Нойманн зі співавторами на порівняльному матеріалі державних організацій показали, що успішність

упровадження ШІ визначається не лише технологічною готовністю, а й інституційною спроможністю організації до змін [18, с. 129–132], а С. Бєлай зі співавторами обґрунтували практико-орієнтовану парадигму управління національною безпекою, що поєднує теоретичний і прикладний рівні аналізу [19]. Л. Сергієнко зі співавторами емпірично підтвердили продуктивність суб'єктного аналізу інституційної архітектури безпекових сфер [20, с. 100–101], що є методологічно застосовним і до аналізу суб'єктів сектору оборони.

Узагальнюючи проаналізовані підходи, можна констатувати: наука державного управління національною безпекою дає категорійний і методологічний апарат [1; 2], дослідження воєнного досвіду доводять технологічну детермінанту трансформації безпекового середовища [3], військово-прикладна література деталізує технічні напрями впровадження ШІ в оборонній сфері [10; 11], а міжнародна та безпекова література розкриває дуальну природу й типологію ШІ-обумовлених загроз [4; 12–17], тоді як ширша література з публічного управління дає інституційну рамку впровадження технологій [18–20]. Жодна з цих праць, однак, не пропонує критеріїв розмежування обороноздатності держави як самостійного об'єкта публічного управління від суміжних категорій оборони й національної безпеки – переважна більшість авторів або ототожнює ці поняття, або взагалі не порушує питання про їх співвідношення. Ця дослідницька прогалина й визначила мету статті.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті – концептуалізувати обороноздатність держави як об'єкт публічного управління та визначити її співвідношення із суміжними категоріями в умовах стрімкого розвитку штучного інтелекту.

Завдання дослідження:

1) Систематизувати наукові підходи до трактування обороноздатності держави, оборони та національної безпеки;
2) Обґрунтувати критерії розмежування обороноздатності держави як самостійного об'єкта публічного управління;
3) Визначити дуальну роль штучного інтелекту в підвищенні обороноздатності держави;
4) Охарактеризувати управлінські імплікації темпоральної асиметрії між розвитком ШІ-технологій і нормотворчим циклом;
5) Зіставити запропоновану концептуалізацію з альтернативними науковими позиціями та визначити межі її застосовності.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для досягнення поставленої мети застосовано системний підхід – для розгляду обороноздатності як багатокомпонентного об'єкта управління; порівняльний метод – для зіставлення її з суміжними категоріями та альтернативними науковими позиціями; контент-аналіз наукових і нормативних джерел – для виявлення критеріїв розмежування понять і верифікації емпіричних прикладів.

Розглядаючи питання розмежування понять обороноздатності, оборони та національної безпеки, аналіз наукового дискурсу дає підстави виокремити ці три категорії за критеріями обсягу та керованості. Оборона – найвужче поняття, що позначає безпосередню військову діяльність держави із захисту суверенітету й територіальної цілісності, законодавчо визначену як функції відповідних органів [3; 10]. Національна безпека – найширша, інтегральна категорія, що охоплює військову, економічну, інформаційну, екологічну та інші складові захищеності державних інтересів [1]. Обороноздатність держави посідає проміжне положення: вона є не військовою дією як такою (оборона) і не станом захищеності в цілому (національна безпека), а сукупністю керованих спроможностей держави – економічних, технологічних, кадрових, управлінських, – які визначають здатність держави протистояти збройній агресії. Саме керованість (а отже, можливість цілеспрямованого публічного управління) відрізняє, на наш погляд, обороноздатність від національної безпеки як ширшої, частково некерованої державою категорії (наприклад, геополітичного середовища) і від оборони як вужчої, суто виконавської діяльності. Узагальнено це розмежування за чотирма критеріями наведено в табл. 1.

Таблиця 1

Розмежування оборони, обороноздатності держави та національної безпеки

Критерій	Оборона	Обороноздатність держави	Національна безпека
Обсяг поняття	найвужче: безпосередня військова діяльність	проміжне: сукупність керованих спроможностей держави	найширше: інтегральна категорія захищеності державних інтересів
Керованість	виконавська діяльність за наказом командування	керовані державою чинники спроможності – об'єкт публічного управління	частково некероване середовище (геополітичний контекст)
Суб'єкт управління	Міністерство оборони, Генеральний штаб (виконавці)	органи публічного управління (плановий, координаційний рівень)	РНБО, увесь сектор безпеки і оборони
Роль штучного інтелекту	інструмент виконання операцій (розвідка, логістика, автономні системи)	керований чинник спроможності, що потребує регулювання	елемент ширшого безпекового середовища, частково некерований

Джерело: систематизовано автором на основі [1; 3; 10; 15]

Дуальна роль штучного інтелекту в підвищенні обороноздатності. Штучний інтелект одночасно розширює керовані спроможності держави й породжує нові класи асиметричних загроз. З одного боку, ШІ-системи підвищують ефективність державних інституцій – зокрема, скорочують строки реагування на запити до 50 % у системі е-Урядування [4] – автоматизують аналіз розвідданих, логістичне планування й кіберзахист критичної інфраструктури, а також відкривають можливості для адаптивних систем управління боєм і гіпермережевої координації різнорідних підрозділів [10]. З іншого боку, задокументована кампанія кібершпигунства, у якій людина-оператор ухвалювала лише ключові стратегічні рішення, тоді як решту операцій виконувала агентна ШІ-система [12], та українська кампанія UAC-0219/WRECKSTEEL, спрямована зокрема проти оборонного профілю критичної інфраструктури [14], демонструють, що ті самі технологічні можливості дозволяють супротивнику автономізувати кібероперації проти оборонної інфраструктури. Аналогічна логіка автономізації застосування сили на міжнародному рівні розглядається Групою урядових експертів ООН з летальних автономних систем озброєнь [16], а П. Шарре показав, що делегування рішень автономним системам є наскрізною проблемою контрольованості, яка не зводиться до конкретного класу озброєнь [15]. Управлінським наслідком цієї дуальності є неможливість підвищення обороноздатності виключно шляхом нарощування ШІ-спроможностей без паралельного розвитку механізмів контролю за їх застосуванням.

Управлінські імплікації темпоральної асиметрії. Цикл оновлення поколінь великих генеративних моделей вимірюється місяцями, тоді як цикл ухвалення й імплементації регуляторних рішень – роками: показовим є досвід еволюції регуляторної бази ЄС від Стратегії кібербезпеки 2013 року через Директиву NIS, Директиву NIS2 (ст. 21) [5] до Регламенту EU AI Act (ст. 6) [9], кожен етап якої концептуально відповідав на виклики попереднього покоління технологій, а не поточного. Структурована база знань MITRE ATLAS, що каталогізує тактики зловмисного використання ШІ за аналогією з матрицею кіберзагроз [13], і дослідницький звіт НАТО про когнітивне протиборство [17] ілюструють, що технічна й безпекова спільноти самостійно виробляють інструментарій швидшого реагування, який випереджає темпи державного нормотворення. На національному рівні ця асиметрія відображена в чинних Стратегії кібербезпеки України [6] та Стратегії інформаційної безпеки [7], тоді як профільна Концепція розвитку штучного інтелекту [8] лише окреслює етапність формування нормативної бази, не встигаючи за фактичною динамікою впровадження ШІ в оборонному секторі. Це вимагає перегляду самої архітектури управління обороноздатністю – з переходом від періодичного перегляду нормативної бази до вбудованої адаптивності та випереджального прогнозування технологічних поколінь.

Запропонована концептуалізація потребує зіставлення з альтернативними позиціями.

По-перше, частина дослідників військово-прикладного напряму [10; 11] розглядає впровадження ШІ в оборонну сферу переважно як технологічну й операційну проблему, не порушуючи питання про статус обороноздатності як об'єкта публічного управління; запропонований у цій статті підхід доповнює цю позицію управлінським виміром, не заперечуючи цінності суто технічного аналізу.

По-друге, О. Нойманн зі співавторами обґрунтовують, що успішність упровадження ШІ в державних організаціях визначається інституційною спроможністю до змін більшою мірою, ніж галузевою специфікою [18]; це узгоджується із запропонованим розмежуванням – керованість, яка відрізняє обороноздатність від національної безпеки, і є проявом такої інституційної спроможності.

По-третє, альтернативною є позиція, що не виокремлює обороноздатність як самостійну категорію, а розглядає її як синонім оборони в широкому сенсі [3]; недоліком такого ототожнення є втрата можливості окремо аналізувати саме керовані, підвладні публічному управлінню чинники спроможності держави, на відміну від суто військово-оперативних аспектів оборони.

Обмеженням запропонованої концептуалізації є те, що критерій керованості потребує подальшої операціоналізації через систему конкретних індикаторів, а її застосовність поза умовами повномасштабної збройної агресії ще не верифікована і потребує детального опрацювання в теоретичній та практичній площинах.

Отже, обороноздатність держави доцільно розглядати як самостійний об'єкт публічного управління, предметна межа якого визначається сукупністю керованих чинників спроможності держави протистояти збройній агресії, а не ототожнювати її з обороною чи національною безпекою. Штучний інтелект, при цьому, виступає технологічною детермінантою, що одночасно розширює ці керовані спроможності й вимагає випереджальної, а не реактивної, трансформації механізмів управління ними.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті обґрунтовано обороноздатність держави як самостійний об'єкт публічного управління, відмінний від оборони й національної безпеки. Систематизовано наукові підходи до трактування цих трьох категорій і встановлено, що обороноздатність посідає проміжне положення між вузьким поняттям оборони як безпосередньої військової діяльності та широкою інтегральною категорією національної безпеки, а критерієм її розмежування є керованість – можливість цілеспрямованого публічного управління відповідними чинниками спроможності держави.

Визначено дуальну роль штучного інтелекту в підвищенні обороноздатності: технології ШІ одночасно розширюють керовані спроможності держави (аналіз розвідданих, логістика, кіберзахист, адаптивні системи управління боєм) і породжують нові класи асиметричних загроз (автономні кібероперації, дипфейки, когнітивний вплив), що унеможливлює підвищення обороноздатності виключно шляхом нарощування ШІ-спроможностей без паралельного розвитку механізмів контролю. Охарактеризовано управлінські імплікації темпоральної асиметрії між циклом оновлення ШІ-технологій і циклом нормотворення на прикладі еволюції регуляторної бази ЄС та України, що обґрунтовує потребу переходу від періодичного перегляду нормативної бази до вбудованої адаптивності управлінських механізмів.

Власне новим результатом є обґрунтування обороноздатності держави як самостійного об'єкта публічного управління за критерієм керованості та визначення її співвідношення з обороною й національною безпекою. Систематизація наукових підходів до трактування суміжних категорій і огляд емпіричних прикладів дуальної природи ШІ є узагальненням наявних у літературі й задокументованих у відкритих джерелах положень, використаним як емпірико-методологічна основа для побудови авторської концептуалізації досліджуваних понять.

Практичне значення отриманих результатів полягає в можливості їх використання для розмежування повноважень між суб'єктами сектору безпеки й оборони, а також для вдосконалення програмних документів у сфері оборонної політики та цифрової трансформації сектору безпеки і оборони України з урахуванням темпоральної асиметрії між технологічним і нормотворчим циклами. Перспективи подальших досліджень пов'язані з операціоналізацією критерію керованості через систему конкретних індикаторів обороноздатності, розробленням типології ШІ-обумовлених загроз обороноздатності держави та механізму управлінського реагування на темпоральну асиметрію між технологічним і нормотворчим циклами, а також з емпіричною верифікацією запропонованої концептуалізації поза умовами повномасштабної збройної агресії.

ЛІТЕРАТУРА:

1. Ситник Г.П. Державне управління національною безпекою України: монографія. Київ: НАДУ, 2012. 408 с.

2. Ліпкан В.А. Національна безпека України: навчальний посібник. Київ: КНТ, 2009. 576 с. ISBN 978-966-373-375-3.

3. Горбулін В., Бадрак В. Війна майбутнього: технологічний вимір. Київ: Bright Books, 2026. ISBN 978-617-7766-88-8.

4. Гаврилечко Ю.В. Інформаційна складова у безпековій політиці держави з огляду на розвиток штучного інтелекту. Сучасний науковий журнал. 2025. № 9(3). С. 16–23. DOI: 10.36994/2786-9008-2025-9-2.

5. 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

6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021

8. 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

9. 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

10. 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. DOI: 10.32782/TNU-2663-6468/2024.6/21.

11. 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.

12. Disrupting the first reported AI-orchestrated cyber espionage campaign. Anthropic. 2025. URL: https://www.anthropic.com/news/disrupting-AI-espionage

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

14. 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

15. 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.

16. 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

17. 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

18. Neumann O., Guirguis K., Steiner R. Exploring artificial intelligence adoption in public organizations: a comparative case study. Public Management Review. 2024. Vol. 26. P. 114–141. https://doi/org/10.1080/14719037.2022.2048685

19. 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. https://doi.org/10.18280/ijsdp.190126

20. Сергієнко Л., Грицишен Д., Вакун О., Дика О., Чиж В. Суб'єктна характеристика систем державного експортного контролю за товарами військового призначення та подвійного використання в країнах Європейського Союзу. Society and Security. 2025. № 6(12). С. 99–107. https://doi.org/10.26642/sas-2025-6(12)-99-107

REFERENCES:

1. Sytnyk, H.P. (2012), Derzhavne upravlinnia natsionalnoiu bezpekoiu Ukrainy [Public administration of Ukraine's national security], monograph, NADU, Kyiv, Ukraine, 408 p. [in Ukrainian].

2. Lipkan, V.A. (2009), Natsionalna bezpeka Ukrainy [National security of Ukraine], textbook, KNT, Kyiv, Ukraine, 576 p., ISBN 978-966-373-375-3. [in Ukrainian].

3. Horbulin, V. and Badrak, V. (2026), Viina maibutnoho: tekhnolohichnyi vymir [The war of the future: the technological dimension], Bright Books, Kyiv, Ukraine, ISBN 978-617-7766-88-8. [in Ukrainian].

4. Havrylechko, Yu.V. (2025), "Informatsiina skladova u bezpekovii polititysi derzhavy z ohliadu na rozvytok shtuchnoho intelektu" [The information component in state security policy in view of the development of artificial intelligence], Suchasnyi naukovyi zhurnal, No. 9(3), pp. 16-23, https://doi.org/10.36994/2786-9008-2025-9-2 [in Ukrainian].

5. 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

6. President of Ukraine (2021), "Decree No. 447/2021 on the Decision of the National Security and Defense Council of Ukraine of 14 May 2021 'On the Cybersecurity Strategy of Ukraine'", available at: https://zakon.rada.gov.ua/laws/show/447/2021 [in Ukrainian].

7. President of Ukraine (2021), "Decree No. 685/2021 on the Decision of the National Security and Defense Council of Ukraine of 15 October 2021 'On the Information Security Strategy'", available at: https://zakon.rada.gov.ua/laws/show/685/2021 [in Ukrainian].

8. Cabinet of Ministers of Ukraine (2020), "Order No. 1556-r 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 [in Ukrainian].

9. 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

10. 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, https://doi.org/10.32782/TNU-2663-6468/2024.6/21 [in Ukrainian].

11. 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, https://doi.org/10.28925/2663-4023.2024.25.161176 [in Ukrainian].

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

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

14. 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 [in Ukrainian].

15. 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.

16. 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

17. 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

18. Neumann, O., Guirguis, K. and Steiner, R. (2024), "Exploring artificial intelligence adoption in public organizations: a comparative case study", Public Management Review, Vol. 26, pp. 114-141, https://doi.org/10.1080/14719037.2022.2048685

19. 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, https://doi.org/10.18280/ijsdp.190126

20. Serhiienko, L., Grytsyshen, D., Vakun, O., Dyka, O. and Chyzh, V. (2025), "Subject characteristics of state export control systems for military and dual-use goods of the European Union countries", Society and Security, No. 6(12), pp. 99-107, DOI: https://doi.org/10.26642/sas-2025-6(12)-99-107

STATE DEFENSE CAPABILITY AS AN OBJECT OF PUBLIC ADMINISTRATION UNDER THE RAPID DEVELOPMENT OF ARTIFICIAL INTELLIGENCE

NEKRIACH Anastasiia, DABIZHA Vira
HEI "Open International University of Human Development "Ukraine"

The article is devoted to conceptualizing state defense capability as an independent object of public administration under the rapid development of artificial intelligence (AI). The relevance of the study stems from the fact that generations of large generative models change faster than legislators and government officials manage to respond, while the concepts of "state defense capability," "defense," and "national security" are largely used as synonyms in the scholarly literature, which complicates forming a clear subject of public administration in this field and delineating authority among subjects of the security and defense sector. The article aims to conceptualize state defense capability as an object of public administration and to determine its correlation with adjacent categories under the proliferation of AI technologies. The study employs the systems approach, the comparative method, and content analysis of scholarly and legal sources. Scholarly approaches to interpreting defense capability, defense, and national security have been systematized. Criteria for their delineation have been substantiated. The dual role of artificial intelligence has been identified – as a tool for enhancing defense capability and as a source of new asymmetric threats. The managerial implications of the temporal asymmetry between the AI technology renewal cycle and the rule-making cycle have been characterized. The proposed

conceptualization has been juxtaposed with alternative scholarly positions. The novelty consists in substantiating state defense capability as an independent object of public administration, distinct from defense and national security, whose subject boundary is defined by a set of governable – rather than merely natural or unconditional – factors of state capacity. The practical significance lies in the applicability of the results to improving policy documents in the field of defense policy and the digital transformation of Ukraine's security and defense sector.

Key words: state defense capability, public administration, artificial intelligence, national security, defense, defense systems, cybersecurity, public authority, state regulation, digitalization.