

Обґрунтування термінологічної системи концептуального документа із запровадження штучного інтелекту в Міністерстві оборони України

Резюме. У статті досліджено вітчизняне законодавство та принципи і підходи НАТО щодо запровадження та використання технологій штучного інтелекту. Стратегічними цільовими програмними документами України закладено підґрунтя запровадження таких технологій у військовій сфері. Початковим кроком для запровадження технологій штучного інтелекту у Міністерстві оборони України є розроблення відповідного концептуального документа, положення якого мають бути спрямовані на подальшу цифрову трансформацію Міністерства оборони України та забезпечення взаємосумісності зі збройними силами держав – членів НАТО. У статті обґрунтовано та запропоновано термінологічну систему як складову частину концептуального документа із запровадження технологій штучного інтелекту у Міністерстві оборони України.

Ключові слова: штучний інтелект; технології штучного інтелекту; термінологічна система; високотехнологічна зброя.

Постановка проблеми. Стрімкий розвиток сучасних інформаційних технологій переміщує людину із матеріального світу у світ віртуальний. На сьогодні важко виокремити сфери діяльності людини, які не охоплені штучним інтелектом (далі – ШІ): медицина, комунікація, освіта, Інтернет, розумний дім, проєктування, література, мистецтво, кібербезпека, юриспруденція, наукові дослідження, енергетика тощо. Цей список сфер людської діяльності, у якому уже широко застосовується ШІ є абсолютно невичерпним та його можливо продовжувати, крім цього, щорічно появляються нові та нові сфери діяльності, у яких використовується ШІ.

Широкомасштабна агресія Російської Федерації проти України стала потужним каталізатором для розвитку передових технологій ШІ в Збройних Силах (далі – ЗС) України. Використання озброєння, військової та спеціальної техніки (далі – ОВТ) із елементами ШІ призводить до збереження найціннішого для нашого війська – життя наших воїнів. У 2024 році “на поле бою прийшли технології, які привів ШІ” [1]. І вже сьогодні лунають все частіше голоси військових фахівців, якими прогнозуються проведення боїв на полі бою (будь-то суходіл чи море) роботизованих комплексів (танків, безпілотних літальних / безкіпажних морських платформ тощо) ворогуючих сторін, управління якими здійснюватиметься як операторами, так і з використанням технологій ШІ. Ураховуючи тенденції застосування та розвитку ОВТ протягом

російсько-української війни зазначене стане реальністю протягом найближчих 5–10 років.

Одним із джерел накопичення у Міністерстві оборони України (далі – Міноборони) практичного досвіду із запровадження технологій ШІ є інноваційний кластер для розвитку військових технологій в Україні “Brave 1” (<https://brave1.gov.ua>), який був запущено у квітні 2023 року.

У контексті глобального технологічного прогресу та триваючого збройного конфлікту технології ШІ можуть бути ключовим інструментом ЗС України з метою підвищення їх оперативної ефективності (оптимізація логістики, аналіз розвідувальних даних), збереження людських ресурсів (використання роботизованих платформ для розмінування чи проведення розвідки, автоматизація медичних діагностичних процесів), посилення обороноздатності (прогнозування дій противника, удосконалення кіберзахисту власних інформаційних систем) тощо.

Питання запровадження технологій ШІ у Міноборони потребує системного підходу та регулювання ряду нормативно-правових питань - через видання документа, яким доцільно визначити концептуальні підходи із зазначеного питання у ЗС України. Такий концептуальний документ, складовою якого має бути відповідна терміносистема, доцільно розробляти з урахуванням положень вітчизняного законодавства як у сфері оборони, так і у галузі ШІ, а також з урахуванням міжнародного досвіду, у т.ч. НАТО. Отже, дослідження терміносистеми в галузі ШІ з урахуванням особливостей

Міністерства оборони України є актуальним питанням.

Аналіз останніх досліджень та публікацій. Поняття ІІІ вперше було введено у 1956 році американським вченим Дж. МакКарті. Бурхливий розвиток технологій ІІІ розпочався близько 10 років тому, хоча базова основа для запровадження технологій ІІІ почала закладатися з 2000-х років після збільшення обчислювальних потужностей комп'ютерів, широкого розповсюдження мережі Інтернет та, внаслідок чого, доступу до великих масивів даних. Також передумовами розвитку технологій ІІІ стали технології хмарних обчислень, які поступово почали витіснити локальні сервери та побудовані на їх основі центри обробки даних, що створило середовище із практично необмеженими обчислювальними спроможностями. Прогрес у розвитку ІІІ продовжує нарощуватися та переріс сподівання своїх засновників. Тому, публікації у галузі ІІІ, яким більше 3-4 років можуть не відображати сучасних тенденцій розвитку сучасних інформаційних технологій.

На сьогодні, видано низку публікацій (підручників), які є підґрунтям для розвитку технологій ІІІ, описують ризики і етичні принципи з їх застосування. Так, у [2] наведена сучасна фундаментальна теорія та практика ІІІ. У [3] розглянуто вплив ІІІ на суспільство та людство, здійснено глибокий аналіз потенційних можливостей та ризиків, пов'язаних з розвитком ІІІ. У [4] досліджено можливі екзистенційні ризики, які пов'язані із розвитком надрозумного ІІІ, запропоновано різного роду стратегії для забезпечення та контролю над розвитком ІІІ, розглянуті етичні виклики. У [5–7] наведені основні поняття та класифікація технологій ІІІ.

Колективом вітчизняних вчених було розроблено монографію, у якій викладена стратегія розвитку ІІІ в Україні протягом 2023 – 2030 років. У монографії визначені пріоритетні (як фундаментальні, так і прикладні та експериментальні) напрями наукових досліджень, завдання і заходи щодо створення та запровадження технологій ІІІ в інтересах економічного й соціального розвитку України. Також зазначено, що одним із пріоритетних напрямів розвитку ІІІ є сфера безпеки та оборони [8].

Ураховуючи прискорене запровадження технологічних рішень, розроблених на основі ІІІ, у різні галузі економіки та сфери суспільних відносин у понад 60-ти державах світу, зокрема і в Україні, протягом останніх років були затверджені стратегії розвитку ІІІ

[9–11], у яких були визначені питання державного регулювання ІІІ, можливості його використання та обмеження у використанні, правове регулювання тощо.

На підставі національних стратегій у високотехнологічних державах світу були затверджені відповідні документи щодо запровадження технологій ІІІ в збройних силах, що у свою чергу принесло відчутні результати. Так, на цей час, збройними силами таких держав уже активно застосовується ІІІ під час модернізації власних бойових, логістичних та інших систем та ОБТ. Такими прикладами можуть бути:

ізраїльська система протиракетної оборони “Залізний купол” [12], у якій використовуються технології ІІІ для виявлення та збиття ракет супротивника;

проведення реорганізації та створення у 2022 році у структурі міністерства оборони США Офісу з цифрової трансформації та штучного інтелекту (*en: Chief Digital and Artificial Intelligence Office, CDAO*), яким здійснюється розроблення та впровадження технологій ІІІ з метою підвищення ефективності структур міністерства оборони, прогнозування потреб і зменшення витрат у військовій логістиці тощо [13].

Ці та інші публікації дають змогу сформувати теоретичні основи та напрями запровадження ІІІ у Міноборони. Однак не повною мірою досліджено вітчизняне законодавство у сфері оборони, що стосується галузі ІІІ. Короткий аналіз такого дослідження може бути включено до концептуального документа ЗС України із запровадження ІІІ. Малодослідженою, також, залишається відповідна термінологія у галузі ІІІ, яка може бути частиною загальноприйнятої загальної військової термінології.

Метою статті є проведення аналізу вітчизняного та закордонного досвіду запровадження і використання технологій ІІІ для обґрунтування та розроблення терміносистеми концептуального документа із запровадження ІІІ у Міністерстві оборони України.

Викладення основного матеріалу. Запровадження технологій ІІІ, які є складовою частиною інформаційних технологій, є невід'ємною частиною розвитку ЗС України. Відсутність концептуальних засад регулювання питань запровадження технологій ІІІ в Міноборони не дає змоги системно здійснювати розвиток ЗС України у цьому напрямі.

На сьогодні, державні стратегічні цільові програмні документи, що стосуються національної та воєнної безпеки [14–16], розроблені до повномасштабного вторгнення Російської Федерації на територію України та не повною мірою враховують наявний прогрес

у застосуванні силами оборони інноваційних технологій на полі бою. Однак їх положення та положення інших нормативних документів можуть бути базовою основою для визначення таких концептуальних засад із запровадження технологій ШІ у силах оборони (рис. 1).

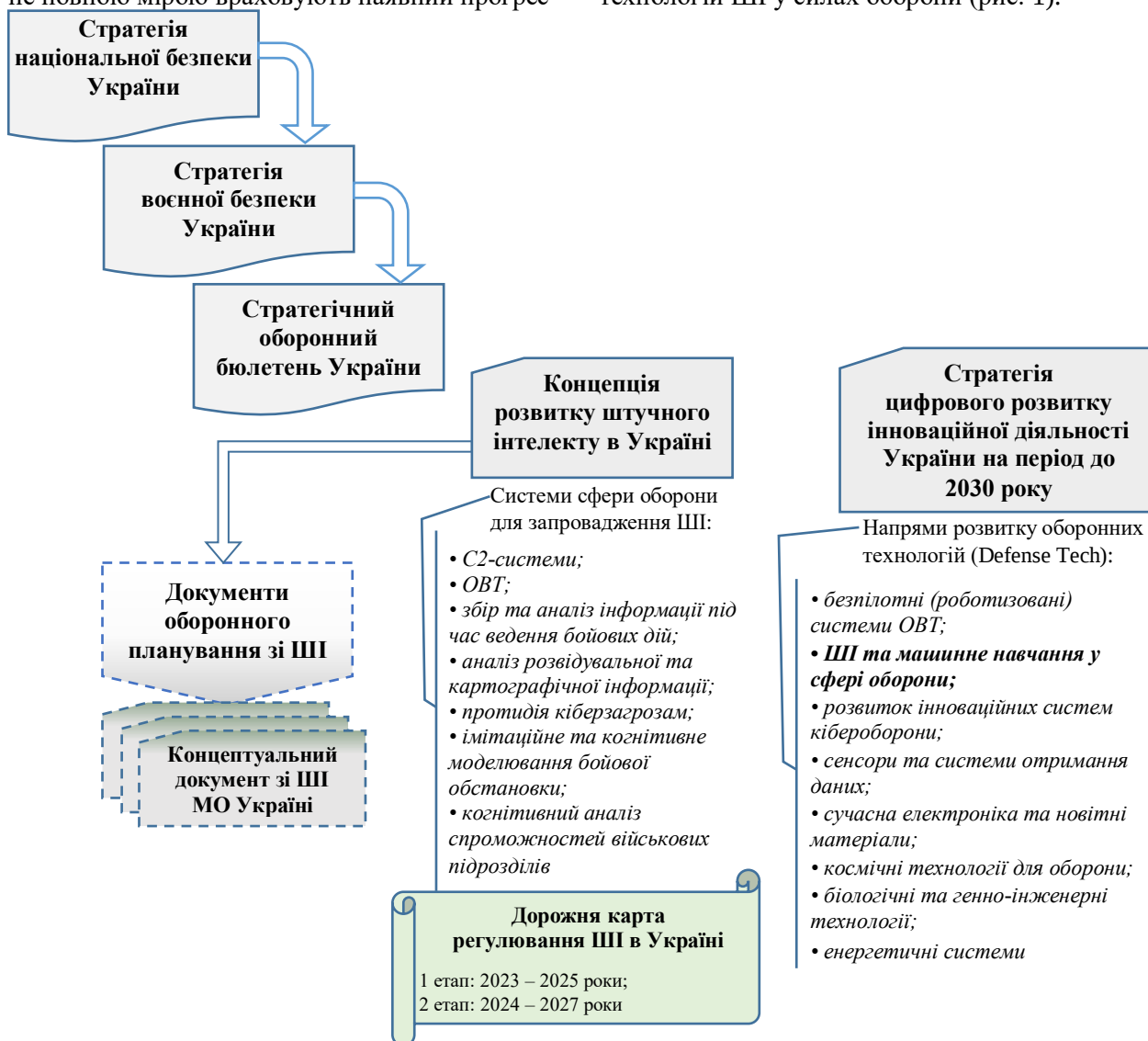


Рис. 1. Нормативно-правові документи щодо запровадження технологій ШІ в Україні

Стратегією національної безпеки України [14] визначено, що зовнішніми прогнозованими загрозами національній безпеці та національним інтересам України є розробки систем озброєнь на основі нових фізичних принципів з використанням технологій в галузі ШІ. Для гарантування безпеки громадян державою мають стимулюватися інновації та запроваджуватися новітні технології, зокрема у сферах безпеки та оборони. У свою чергу, зміцнення бойового потенціалу ЗС України має здійснюватися шляхом удосконалення і розвитку на основі сучасних технологій систем управління, електронних комунікацій, розвідки, логістики та оснащення новими, зокрема

високотехнологічними, зразками ОВТ. Інвестування у розвиток технологій повинно здійснюватися оборонно-промисловим комплексом. До того ж державою вживатимуться відповідні заходи щодо зміцнення потенціалу оборонно-промислового комплексу.

Основою Стратегії воєнної безпеки України [15] є всеохоплююча оборона України, яка передбачає підтримання балансу та синергії воєнних і невоєнних засобів для забезпечення воєнної безпеки України, зокрема: використання новітніх високотехнологічних і вискоефективних засобів ведення збройної боротьби. Для досягнення синергії ЗС України потрібно

комплектувати професійним особовим складом та оснащувати сучасним високотехнологічним озброєнням, військовою та спеціальною технікою: високоточними засобами ураження, безпілотними платформами (системами) наземного, морського та повітряного базування, космічною технікою військового (подвійного) призначення. Указане потребує впровадження сучасних інформаційних технологій, цифровізацію управлінських процесів і різних галузей діяльності, державною підтримкою оснащення ЗС України новим озброєнням.

Стратегічним оборонним бюлетенем України [16] визначені основні напрями реалізації воєнної політики України в контексті всеохоплюючої оборони України. Одним з таких основних напрямів є розвиток спроможностей сил оборони в контексті підготовки до ведення всеохоплюючої оборони України. Розвиток існуючих та формування перспективних спроможностей ЗС України здійснюється відповідно до визначених стратегічних цілей. Аналіз цих стратегічних цілей показує, що запровадження технологій ІІІ є доцільним для досягнення очікуваного результату практично кожної стратегічної цілі.

Наприклад, у Стратегічній цілі 1, очікуваним результатом якої є поєднані та інтегровані процеси організації всеохоплюючої оборони, об'єднаного керівництва та оборонного менеджменту, технології ІІІ можливо запровадити під час планування розвитку оборонних спроможностей шляхом застосування математичних методів моделювання, керування ресурсами тощо. Очікуваним результатом виконання завдання 1.5 цієї Стратегічної цілі 1 передбачено здійснити цифрову трансформацію діяльності системи Міноборони, запровадити сучасні інформаційні технології у системи управління військами та зброєю, створення єдиного інформаційного середовища сил оборони.

Очікуваним результатом Стратегічної цілі 2 передбачено переведення ЗС України на професійну основу, вмотивований особовий склад яких підтримується за рахунок ефективних та прозорих систем кадрового менеджменту, військової освіти, охорони здоров'я і соціального захисту. Побудову вказаних ефективних систем із використанням різних мотиваційних чинників доцільно здійснювати із використанням технологій ІІІ.

Стратегією цифрового розвитку інноваційної діяльності України на період до

2030 року [17] визначена візія щодо державної політики у сфері цифрового розвитку інноваційної діяльності. Стратегією визначені відповідні стратегічні цілі. Досягнення цілей заплановано здійснювати відповідно до операційного плану заходів та поетапно. На першому етапі (протягом 2025–2027 рр.) передбачено удосконалення нормативної бази, підтримку наукових досліджень і розробок, розвиток необхідної інфраструктури. За результатами виконання першого етапу заплановано розробити план заходів другого етапу на 2028 – 2030 роки. Запровадження технологій ІІІ визначено у Стратегічній цілі 16, для досягнення якої визначено низку завдань, серед яких: створення інноваційного кластера ІІІ, створення регуляторної платформи для тестування високотехнологічних продуктів на основі ІІІ, поступовий перехід на стандарти, визначені у законодавстві Європейського Союзу (далі – ЄС) тощо.

На підставі положень вказаної Стратегії [17] Міністерством цифрової трансформації України (далі – Мінцифри), яке є ключовою державною структурою у розвитку та запровадженні технологій ІІІ в Україні, запропоновані ключові сфери діяльності, які є основою розвитку інновацій протягом найближчих 5 років [18]. Однією з таких сфер є оборонні технології (DefenseTech), основні напрями їх розвитку наведено на Рис. 1. Технології ІІІ та машинного навчання у сфері оборони є одним із основних напрямів інноваційного розвитку.

Концепцією розвитку штучного інтелекту в Україні [19] визначено пріоритетні сфери діяльності для реалізації в них технологій ІІІ. Однією з таких сфер є сфера оборони, для якої також визначені системи сфери оборони для запровадження в них технологій ІІІ (рис. 1). Також, цією Концепцією зазначено, що пріоритетні напрями і основні завдання з розвитку технологій ІІІ у сфері оборони повинні визначатися у відповідних документах оборонного планування. Такі документи у Міноборони відсутні.

Дорожньою картою регулювання ІІІ в Україні, презентованою Мінцифрою у жовтні 2023 року, запропоновано здійснити поетапне (*I* – 2023–2025 рр.; *II* – 2024–2027 рр.) запровадження механізмів регулювання ІІІ в Україні [20]. Результатом виконання Дорожньої карти є запровадження 50 % положень законодавчого акту ЄС із регулювання ІІІ. У рамках виконання цієї

Дорожньої карти Мінцифрою із залученням ряд заходів, які наведено у Табл. 1.
зацікавлених сторін організовано / проведено

Таблиця 1

Основні заходи із запровадження ШІ в Україні

Термін	Короткий опис заходу
Жовтень 2024 року	Запроваджено експериментальний проєкту щодо організації проведення дослідження високотехнологічних засобів методом “Sandbox” [21]. <i>Довідка. Метод “Sandbox” є сукупністю заходів, що дають змогу провести дослідження високотехнологічних засобів, що використовують ШІ, у захищеному середовищі для їх повноцінного використання на предмет безпечності, відповідності законодавству, стандартам, а також патентної чистоти, дотримання прав інтелектуальної власності, встановлення ринкової затребуваності.</i> <i>У межах вказаного проєкту у лютому 2025 року Міноборони ініціювало створення інноваційної платформи для впровадження новітніх технологій розмінування деокупованих територій. Ця платформа об’єднує зусилля різних зацікавлених сторін для тестування та впровадження ефективних рішень у сфері безпеки</i>
Грудень 2024 року	Мінцифри презентувало узагальнений словник термінів у сфері ШІ [22]. Словник містить 106 юридичних та технічних термінів та словосполучень, які подані з англійським відповідником і визначенням. У цьому Словнику під терміном “<i>штучний інтелект</i>” у контексті галузі ШІ розуміється загальна назва сукупності інформаційних технологій, як-от алгоритмів, методів, підходів, моделей та сервісів, що займаються створенням та розвитком інтелектуальних систем, здатних виконувати завдання, які зазвичай потребують людського інтелекту
Лютий 2025 року	Запущено Центр передового досвіду з розроблення та інтеграції ШІ (AI Center of Excellence), для якого визначили такі завдання [23–24]: - розроблення продуктів ШІ в інтересах державних органів та сектору безпеки і оборони; - аналіз нормативно-правових актів із використанням ШІ; - адаптація європейського законодавства та цифрова експертиза; - упровадження ШІ в науку; - створення освітніх можливостей для спеціалістів ШІ та громадян; - підтримка стартапів, малих і середніх підприємств в інтеграції ШІ; - співпраця з міжнародними технологічними компаніями (BigTech). Мінцифри запустило безоплатний практичний серіал про ChatGPT на Дія.Освіта [25]
Березень 2025 року	Мінцифрою спільно з зацікавленими сторонами розроблено для публічних службовців рекомендації про ефективне та безпечне використання ШІ в роботі [26]. Документ містить практичні пропозиції щодо використання ШІ в органах державної влади та місцевого самоврядування: підготовка звітів відповідей на звернення громадян за допомогою ШІ, аналіз законодавства й прораховування наслідків тих чи інших рішень

Стратегія НАТО. Слід, зауважити, що державами – членами Організації Північноатлантичного договору приділяється значна увага питанню використання спроможностей ШІ та їхньому прагненню адаптуватися до швидкого розвитку технологій, у т.ч. їх впливу на оборону й безпеку. Так, у липні 2024 року було опубліковано оновлену Стратегію НАТО зі ШІ [27]. Ця оновлена Стратегія базується на перегляді попередньої Стратегії НАТО зі ШІ 2021 року, зберігаючи її візію, але адаптуючи її до нових викликів і можливостей, та відображає еволюцію підходу НАТО до використання ШІ у сфері оборони. У Стратегії підкреслено про швидкий розвиток технологій ШІ, зокрема генеративного ШІ, який здатен створювати складні тексти, програмні коди, зображення та аудіо у величезних обсягах, що майже не відрізняються від людської діяльності. Альянсом визнається необхідність якомога швидшого впровадження таких технологій там, де це доцільно, з метою збереження стратегічної переваги та

підвищення ефективності операцій, аналізу даних і прийняття рішень.

Ключовою частиною стратегії є чотири цілі та шість результатів, які спрямовані на інтеграцію ШІ в оборонні системи Альянсу. НАТО наголошує на шести принципах відповідального використання ШІ у сфері оборони: законність (*en: Lawfulness*), відповідальність (*en: Responsibility*) і підзвітність (*en: Accountability*), пояснюваність (*en: Explainability*) і відстежуваність (*en: Traceability*), надійність (*en: Reliability*), керованість (*en: Governability*) та зменшення упередженості (*en: Bias Mitigation*). Ці принципи покликані забезпечити етичне та безпечне застосування технологій ШІ в межах Альянсу. Стратегія визнає, що широка доступність ШІ, зокрема генеративних моделей, створює як можливості, так і ризики, включно з потенційними загрозами від супротивників.

Оновлена стратегія відображає прагнення НАТО адаптуватися до змін у високотехнологічному ландшафті, де конкуренція у галузі ШІ набуває

геополітичного значення. Вона підкреслює важливість інновацій для підтримання колективної оборони та реагування на нові загрози. Порівняно з 2021 роком, в оновленій стратегії акцентується увага на практичному запровадженні технологій ІІІ, а не лише на теоретичних засадах його регулювання. Це свідчить про перехід НАТО від планування використання ІІІ до практичних кроків реалізації.

Слід також зауважити, що в НАТО було приділено увагу стандартизації термінології у сфері інформаційних технологій. Результатом цього стало прийняття у 2005 році угоди зі стандартизації НАТО (*en: STANdardization AGreement, STANAG*): STANAG 5625. Вказаною угодою запроваджено відповідну союзну публікацію ADatP-02. NATO Information Technology Glossary (*укр: Словник НАТО з інформаційних технологій*). У цій публікації наведено термінологію у галузі ІІІ, як складову термінології у сфері інформаційних технологій. Протягом 2023–2025 рр. вказані угода та публікація НАТО були прийняті у якості військового стандарту ВСТ 600.005, який складається із 7 частин. Проблемним питанням цих документів щодо термінології у галузі ІІІ є те, що з 2005 року до вказаної публікації зміни не вносились, тому низка термінів і визначень є застарілими та не ураховують питання розвитку галузі ІІІ сьогодення [28].

Міжнародна стандартизація. У 2017 році на базі Міжнародної організації зі стандартизації (*en: International Organization for Standardization, ISO*) та із залученням представників Міжнародної електротехнічної комісії (*en: International Electrotechnical Commission, IEC*) було створено спільний підкомітет ISO/IEC JTC 1/SC 42 “Artificial intelligence”, на який покладено завдання із розроблення міжнародних стандартів, технічних рапортів та технічних специфікацій у галузі ІІІ. На сьогодні цим підкомітетом розроблено 34 стандарти та знаходяться в різних стадіях розроблення ще

40 стандартів [29]. Одним з цих стандартів є виданий у 2022 році міжнародний стандарт ISO/IEC 22989, яким визначено термінологію у галузі ІІІ [30]. В Україні цей стандарт не запроваджено як національний стандарт.

Отже, враховуючи вітчизняне законодавство у сфері оборони та галузі ІІІ, принципи та підходи НАТО у цій сфері, широкомасштабну збройну агресію, направлену проти України, досвід, отриманий вітчизняними виробниками ОВТ із використанням ІІІ та ЗС України у використанні такого ОВТ, стрімкий прогрес у розвитку технологій ІІІ, з метою системного підходу та регулювання питань в галузі ІІІ у Міноборони потребує розроблення концептуальний документ (концепція, візія тощо) із запровадження технологій ІІІ у сфері оборони. Такий концептуальний документ має задовольняти вимогам:

бути прагматичним та орієнтованим на майбутнє, але водночас ураховувати майбутні ризики;

демонструвати готовність Міноборони до технологічної еволюції, зберігаючи при цьому фокус на етичних стандартах і всеохоплюючій обороні;

не розкривати технічних деталей, залишаючи простір для гнучкості в реалізації;

бути основою для розроблення інших нормативних документів та військових стандартів за напрямками ІІІ;

ураховувати співпрацю з НАТО та ЄС, та у перспективі інтеграцію України в ці структури.

Наведений аналіз законодавства України доцільно включити до цього концептуального документа. Концептуальний документ має містити основні терміни і визначення, які складуть базову термінологію для формування терміносистеми у галузі ІІІ у Міноборони. Вказана термінологія має відповідати принципам, які наведені у Табл. 2:

Таблиця 2

Основні принципи формування терміносистеми із запровадження ІІІ в Міноборони

Принцип	Короткий опис
Чіткість і однозначність	ЗС України потребують високої точності у формулюваннях. Визначення термінів повинні бути усталеними україномовними відповідниками у науковій та технічній літературі англomовних термінів, зрозумілими відповідним зацікавленим сторонам, таким як, замовники та розробники ОВТ та програмних застосунків, оперативний та технічний персонал тощо
Функція освіти	Концептуальний документ може бути використаний особами, які приймають рішення (командування органів військового управління або військових частин, політичні особи), а не лише технічним персоналом та фахівцями, якими використовуються ОВТ з елементами ІІІ. Також така термінологія допоможе таким особам краще зрозуміти сутність технології
Стандартизація	У контексті інтеграції України до європейських та євроатлантичних структур введення термінів сприятиме уніфікації підходів до запровадження ІІІ в системі Міноборони
Контекстуалізація	Визначення термінів дозволять адаптувати загальні поняття ІІІ до специфіки ЗС України, підкреслюючи їхнє прикладне значення

Ураховуючи зазначене, в Табл. 3 наведено базову термінологію – набір термінів та їх визначень, які доцільно включити до концептуального документа, та який розмістити в окремому розділі “Основні терміни та визначення” або додатку, щоб не перевантажувати основний текст. До того ж, наведення вузькотехнічних та спеціальних

термінів доцільно здійснювати у відповідних військових стандартах або інших нормативних документах (методичних рекомендаціях тощо), які доцільно розробити за результатами затвердження концептуального документа. До кожного запропонованого терміну надано роз’яснення щодо його застосування у Міноборони.

Таблиця 3

Термінологічна система у галузі штучного інтелекту у Міноборони (загальні поняття)

Термін	Визначення*
Терміни “штучний інтелект” і “галузь штучного інтелекту” та їх визначення використати з урахуванням положень Концепції розвитку ШІ в Україні [19]	
Штучний інтелект, ШІ (en: Artificial Intelligence, AI)	(Як інструмент) Організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань. У стратегічному контексті ШІ є інструментом для посилення спроможностей сил оборони через цифровізацію розвідки, планування та управління операціями. Додаткові визначення: [30]: (як наукова дисципліна) дослідження та розроблення механізмів і застосувань систем ШІ. <i>Примітка:</i> Дослідження та розроблення можуть відбуватися в будь-якій кількості галузей, таких як комп’ютерні науки, наука про дані, гуманітарні науки, математика та природничі науки. [22]: (як галузь) загальна назва сукупності інформаційних технологій, як-от алгоритмів, методів, підходів, моделей та сервісів, що займаються створенням та розвитком інтелектуальних систем, здатних виконувати завдання, які зазвичай потребують людського інтелекту
Галузь штучного інтелекту	Напрямок діяльності у сфері інформаційних технологій, який забезпечує створення, впровадження та використання технологій штучного інтелекту
Машинне навчання (en: Machine Learning, ML)	Напрямок ШІ, який дає змогу системам удосконалювати свою продуктивність шляхом аналізу даних без явного програмування. У силах оборони – основа для прогнозування загроз, аналізу великих обсягів розвідувальних даних і оптимізації ресурсів У контексті сфери оборони може застосовуватися для аналізу великих обсягів розвідувальних даних, прогнозування поведінки противника чи оптимізації логістики (ресурсів). Додаткові визначення: [30]: підхід до створення багатих ієрархічних представлень шляхом тренування нейронних мереж із багатьма прихованими шарами; [22]: галузь ШІ, що навчається приймати рішення, налаштовуючи параметри математичних моделей відповідно до даних спостереження
Глибоке навчання (en: Deep Learning, DL)	Напрямок машинного навчання, що використовує нейронні мережі з багатьма шарами для обробки складних даних, таких як зображення, звук чи текст. У контексті сфери оборони може застосовуватися для розпізнавання цілей, аналізу відеопотоків із роботизованих комплексів чи виявлення аномалій. Додаткові визначення: [30]: процес оптимізації параметрів моделі за допомогою обчислювальних технік таким чином, щоб поведінка моделі відображала дані або досвід; [22]: галузь машинного навчання, яка присвячена тренуванню моделей, таких як нейронні мережі, що складаються з багатьох шарів
Нейронна мережа (en: Neural Network, NN)	Математична модель, що імітує роботу людського мозку для обробки інформації. У контексті сфери оборони може застосовуватися як основа для систем розпізнавання образів, обробки сигналів чи автономних систем. Додаткові визначення: [30]: мережа, що складається з одного або більше шарів нейронів, з’єднаних зваженими зв’язками з регульованими вагами, яка приймає вхідні дані та генерує вихідні дані; [22]: модель, яка складається з одного або кількох шарів штучних нейронів, з’єднаних зваженими зв’язками з ваговими коефіцієнтами. Нейронна мережа перетворює вхідні дані,

ІНФОРМАТИЗАЦІЯ ЗБРОЙНИХ СИЛ

Термін	Визначення*
	пропускаючи їх через себе, при цьому кожен нейрон виконує прості обчислення
Обробка природної мови (en: Natural Language Processing, NN)	Технологія та один із напрямів ШІ, яка дозволяє комп'ютерам розуміти, інтерпретувати та генерувати людську мову. У контексті сфери оборони може застосовуватися для аналізу розвідувальних даних, здійснення оперативного перекладу, моніторингу інформаційного простору, створення командних інтерфейсів, розпізнавання та транскрипції мовлення. Додаткові визначення: [30]: наукова дисципліна, що стосується способів, якими системи отримують, обробляють та інтерпретують природну мову; [22]: напрям ШІ, який зосереджується на обробці, аналізі та генеруванні людської мови
Комп'ютерний зір (en: Computer vision)	Технологія та один із напрямів ШІ, що забезпечує спроможність систем ШІ отримувати, обробляти та інтерпретувати візуальні дані, такі як зображення або відео, імітуючи людське сприйняття. У контексті сфери оборони може застосовуватися для аналізу розвідувальних даних (зображень супутників, камер спостережень, дронів) та зони бойових дій, розпізнавання цілей, автономного виконання завдань роботизованими платформами, моніторингу лінії бойового зіткнення, виявлення ворожих безпілотників. Додаткові визначення: [30]: спроможність функціонального блоку отримувати, обробляти та інтерпретувати дані, що представляють зображення або відео; Примітка. Комп'ютерний зір передбачає використання сенсорів для створення цифрового зображення візуальної картинки. Це може включати зображення, такі як зображення, що фіксують довжини хвиль за межами видимого світла, наприклад, інфрачервоне зображення. [22]: напрям ШІ, який зосереджується на обробці, аналізі та генеруванні візуальної інформації (зображень, відео тощо)
Автономна система (en: Autonomous System)	Технологічна система, здатна виконувати завдання без постійного людського контролю завдяки інтеграції ШІ. У контексті сфери оборони під автономними системами розуміються безпілотні літальні / безкіпажні морські платформи, роботизовані платформи чи системи протиповітряної оборони Додаткові визначення: [30]: автономність, автономний (en: Autonomy, Autonomous) – характеристика системи, яка спроможна змінювати свою передбачену сферу використання або мету без зовнішнього втручання, контролю чи нагляду; Довідка. Автономність є ключовою характеристикою системи ШІ, що підкреслює їхню здатність до саморегуляції та адаптації. [22]: властивість системи ШІ, що полягає в її здатності функціонувати самостійно без втручання людини
Велика мовна модель (en: Large language Model, LLM)	Технологія ШІ, здатна інтерпретувати контекст введеного тексту та генерувати відповіді чи продовження природною мовою, спираючись на знання, отримані під час навчання на текстових масивах даних. У контексті сфери оборони може застосовуватися для генерування оперативних зведень на основі розвідувальних даних, моделювання діалогів для проведення інформаційних операцій (дезінформація), аналіз перехоплених повідомлень для виявлення загроз. Додаткові визначення: у [30] термін не виділено як окремий з власним визначенням, але він належить до загальної категорії моделей ШІ, які навчаються на великих наборах даних для виконання мовних завдань; [22]: клас мовних моделей, які використовують алгоритми глибокого навчання та навчаються на великих наборах даних, котрі можуть містити не тільки текст, але й інші модальності (зображення, аудіо тощо)

Примітка. У таблиці наведені додаткові визначення термінів із зазначенням джерел інформації.

Висновки. Технології ШІ являють собою не лише сучасні інформаційні технології, що можуть бути застосовані у різних галузях економіки, а і є новим підходом до обробки різних даних (природної мови, зображень, тексту, відео тощо), які можуть бути використані у сфері оборони та запровадження яких у Міноборони дозволить

нарастити спроможності ЗС України, підвищити ефективність їх застосування під час оборони держави в умовах постійно змінюваної обстановки на полі бою оптимізуючи процеси прийняття рішень з урахуванням ситуаційної обізнаності.

Проведений аналіз вітчизняного законодавства свідчить про доцільність

запровадження технологій ШІ у Міноборони. Сфера безпеки і оборони є одним із важливих напрямів розвитку ШІ. Підтвердженням вказаного є, також, підходи НАТО з цього питання. Також одним з важливих аргументів розроблення та застосування високотехнологічного озброєння із елементами ШІ є отриманий силами оборони практичний досвід на полі бою.

Для регулювання питань розвитку технологій ШІ з урахуванням сучасної безпекової ситуації доцільно розробити концептуальний документ із запровадження технологій ШІ в Міноборони, який буде наступним інструментом із цифрової трансформації системи Міноборони, що забезпечить технологічну перевагу над противником не лише у кіберпросторі, але й в інших просторах (доменах): на суходолі, морі та повітрі. До того ж запровадження єдиної та зрозумілої для всіх зацікавлених сторін терміносистеми має бути передувати початковому етапу запровадження технологій ШІ у Міноборони. Запропонована у статті терміносистема є одним із таких інструментів.

Подальші дослідження доцільно зосередити на дослідженні спроможностей технологій ШІ для ресурсного забезпечення військ (сил) зразками озброєння, військової та спеціальної техніки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Виступ Залужного: з генералами НАТО ніхто не розмовляв так жорстко. 19 жовтня 2024 року. URL: <https://glavcom.ua/columns/mknyazhitsky/vistup-zaluzhnoho-z-heneralami-nato-nikhto-ne-rozmovljav-tak-zhorstko-1026693.html> (дата звернення: 20.03.2025).
2. Рассел С., Норвіг П. Штучний інтелект: сучасний підхід. 4-те видання. Том 1. Рішення проблем: знання і міркування. Діалектика, 2021. 706 с.
3. Тегмарк М. Життя 3.0: бути людиною в епоху штучного інтелекту. Київ : Наш формат, 2019. 432 с.
4. Бостром Н. Суперінтелект. Стратегії і небезпеки розвитку розумних машин. Київ : Наш формат, 2020. 408 с.
5. Understanding the different types of artificial intelligence. 12.10.2023. URL: <https://www.ibm.com/think/topics/artificial-intelligence-types> (дата звернення: 20.03.2025).
6. What Is Artificial Intelligence? Definition, Uses, and Types. 19.12.2024. URL: <https://www.coursera.org/articles/what-is-artificial-intelligence> (дата звернення: 20.03.2025).
7. Штучний інтелект (ШІ) – що це таке, як працює і навіщо потрібен. URL: <https://termin.in.ua/shtuchnyy-intelekt> (дата звернення: 20.03.2025).
8. Стратегія розвитку штучного інтелекту в Україні : монографія / за ред. А. І. Шевченка. Київ : Наука і освіта, 2023. 305 с. DOI: https://doi.org/10.15407/development_strategy_2023 (дата звернення: 20.03.2025).
9. Андрощук Г. О. Політика і стратегії розвитку штучного інтелекту в країнах світу: quo vadis? (Частина 1) // Наука, технології, інновації. 2023. № 1 (25). С. 15–29. DOI: <http://doi.org/10.35668/2520-6524-2023-1-03> (дата звернення: 20.03.2025).
10. Андрощук Г. О. Політика і стратегії розвитку штучного інтелекту в країнах світу: quo vadis? (Частина 2) // Наука, технології, інновації. 2023. № 2 (26). С. 40–47. DOI: <http://doi.org/10.35668/2520-6524-2023-2-05> (дата звернення: 20.03.2025).
11. Костенко О. В. Аналіз національних стратегій розвитку штучного інтелекту. Інформація і право. 2022. № 2 (41). С. 58–69. DOI: [https://doi.org/10.37750/2616-6798.2022.2\(41\).270365](https://doi.org/10.37750/2616-6798.2022.2(41).270365) (дата звернення: 20.03.2025).
12. Негіна В. Р., Слісаренко О. М. Штучний Інтелект: особливості правового регулювання (на прикладі Держави Ізраїль) // Юридичний науковий електронний журнал. 2024. № 4. С. 696–699. DOI: <https://doi.org/10.32782/2524-0374/2024-4/166> (дата звернення: 20.03.2025).
13. Офіційний веб-сайт Офісу з цифрової трансформації та штучного інтелекту Міністерства оборони США. URL: <https://www.ai.mil> (дата звернення: 20.03.2025).
14. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України” : Указ Президента України від 14.09.2020 № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 20.03.2025).
15. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України” : Указ Президента України від 25.03.2021 № 121/2021. URL: <https://www.president.gov.ua/documents/1212021-37661> (дата звернення: 20.03.2025).
16. Про рішення Ради національної безпеки і оборони України 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України” : Указ Президента України від 17.09.2021 № 473. URL: <https://www.president.gov.ua/documents/4732021-40121> (дата звернення: 20.03.2025).
17. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках : розпорядження Кабінету Міністрів оборони України від 31.12.2024 № 1351-р. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> (дата звернення: 20.03.2025).
18. WINWIN: Україна затвердила Стратегію цифрового розвитку інновацій до 2030 року. 14.02.2025. URL: <https://thedigital.gov.ua/news/winwin-ukraina-zatverdila-strategiyu-tsifrovogo->

- rozvitku-innovatsiy-do-2030-roku (дата звернення: 20.03.2025).
19. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. Дата оновлення: 29.12.2021. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n7> (дата звернення: 20.03.2025).
 20. Регулювання штучного інтелекту в Україні: презентуємо дорожню карту. 07.10.2023. URL: <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu> (дата звернення: 20.03.2025).
 21. Про реалізацію експериментального проекту щодо організації проведення дослідження високотехнологічних засобів методом “Sandbox”: Постанова Кабінету Міністрів оборони України від 29.10.2024 № 1238. URL: <https://zakon.rada.gov.ua/laws/show/1238-2024-%D0%BF#Text> (дата звернення: 20.03.2025).
 22. Як говорити про штучний інтелект: знайомтеся зі словником термінів. 26.12.2024. URL: <https://thedigital.gov.ua/news/yak-govoriti-pro-shtuchniy-intelekt-znayomtesya-zi-slovnikom-terminiv> (дата звернення: 20.03.2025).
 23. Мінцифра запускає WINWIN AI Center of Excellence – центр передового досвіду з розробки та інтеграції ІІІ. 04.02.2025. URL: <https://thedigital.gov.ua/news/mintsifra-zapuskae-winwin-ai-center-of-excellence-tsentr-peredovogo-dosvidu-z-rozrobki-ta-integratsii-shi> (дата звернення: 20.03.2025).
 24. У Мінцифри запустили Центр штучного інтелекту в Україні: що це, для чого та хто очолить. 05.02.2025. URL: https://24tv.ua/shtuchniy-intelekt-diyi-mintsifra-zapustila-tsentr-shi-ukrayini_n2745566 (дата звернення: 20.03.2025).
 25. Як робити більше за короткий час: Мінцифра запустила безоплатний практичний серіал про ChatGPT на Дія.Освіта. 27.02.2025. URL: <https://thedigital.gov.ua/news/yak-robiti-bilshe-zakorotshiy-chas-mintsifra-zapustila-bezoplatniy-praktichniy-serial-pro-chatgpt-na-diyaosvita> (дата звернення: 20.03.2025).
 26. Як перетворити ІІІ на власного помічника – поради для публічних службовців. 14.03.2025. URL: <https://thedigital.gov.ua/news/yak-peretvoriti-shi-na-vlasnogo-pomichnika-poradi-dlya-publichnikh-sluzhbovtiv> (дата звернення: 20.03.2025).
 27. Summary of NATO's revised Artificial Intelligence (AI) strategy. 10.07.2024. URL: https://www.nato.int/cps/en/natohq/official_texts_227237.htm (дата звернення: 12.03.2025).
 28. Електронна база військових стандартів України. URL: <https://milstand.knu.ua> (дата звернення: 20.03.2025).
 29. Веб-сторінка підкомітету ISO/IEC JTC 1/SC 42 “Artificial intelligence”. URL: <https://www.iso.org/committee/6794475.html> (дата звернення: 20.03.2025).
 30. International standard ISO/IEC 22989 :2022(E). Information technology – Artificial intelligence – Artificial intelligence concepts and terminology. First edition 2022-07. 70 p.

Стаття надійшла до редакційної колегії 21.03.2025

Justification of the terminological system of the conceptual document on the introduction of artificial intelligence in the Ministry of Defense of Ukraine

Annotation

The rapid development of modern information technologies is shifting humanity from the material world to the virtual one. Today, it is difficult to distinguish areas of human activity that are not influenced by artificial intelligence (AI), including medicine, communication, education, the Internet, smart homes, design, literature, art, cybersecurity, law, scientific research, energy, and more.

In the context of global technological progress and the ongoing armed conflict, artificial intelligence (AI) technologies may become a key tool for the Armed Forces of Ukraine to enhance their operational efficiency (logistics optimization, intelligence data analysis), preserve human resources (use of robotic platforms for demining or reconnaissance, automation of medical diagnostic processes), and strengthen defense capabilities (predicting enemy actions, improving the cybersecurity of their information systems), among other applications.

This article examines national legislation and NATO principles and approaches regarding the introduction and use of artificial intelligence technologies. Ukraine's strategic program documents have laid the groundwork for the introduction of such technologies in the military sphere.

The initial step for implementing artificial intelligence technologies in the Ministry of Defense of Ukraine is the development of an appropriate conceptual document, the provisions of which should aim at further digital transformation of the Ministry of Defense of Ukraine and ensuring interoperability with the armed forces of NATO member states.

The article substantiates and proposes a terminology system as an integral part of the conceptual document for introducing artificial intelligence technologies in the Ministry of Defense of Ukraine.

Keywords: artificial intelligence; artificial intelligence technologies; terminological system; high-tech weapons.