

Гмиря Вікторія, Романовська Людмила, Нікітченко Анна, Панченко Антон. Розділ III. Переваги та виклики використання штучного інтелекту у галузі оборони. Штучний інтелект у науці : монографія / [авт. колектив]; за ред. Яцишина Андрія та Яцишин Анни. – Київ: ФОП Ямчинський О.В., 2025. – С. 44-59. ISBN 978-617-8830-09-0

РОЗДІЛ III. ПЕРЕВАГИ ТА ВИКЛИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ГАЛУЗІ ОБОРОНИ

DOI: 10.33407/lib.NAES.id/748232

Гмиря Вікторія^{1[0000-0003-3070-0158]}, **Романовська Людмила**^{1[0009-0002-7284-1493]},
Нікітченко Анна^{1[0000-0001-9387-5639]}, **Панченко Антон**^{1[0009-0003-9254-6464]}

¹Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна

Анотація. Міжнародний досвід війн останніх років свідчить, що сучасні бойові дії характеризуються високою інтенсивністю та динамікою. Це спричиняє значні потоки інформації, обробка яких і швидке ухвалення рішень потребують значних зусиль і часу, адже необхідно враховувати велику кількість змінних факторів. Стрімка зміна обстановки на полі бою вимагає не лише оперативного, а й завчасного реагування та прогнозування можливих сценаріїв розвитку подій. Водночас людський фактор складність ухвалення швидких та ефективних рішень може істотно впливати на хід бойових дій. У таких умовах впровадження алгоритмів штучного інтелекту сприяє розв'язанню складних і потенційно небезпечних завдань, а також підвищує ефективність застосування зброї. Технологічні інновації у поєднанні зі штучним інтелектом стають ключовим чинником успіху в сучасній війні. Тому дослідження, спрямовані на їхній розвиток, мають надзвичайно важливе значення.

Ключові слова: штучний інтелект, війна, кібербезпека, масив даних, оборона.

ADVANTAGES AND CHALLENGES OF MILITARY ARTIFICIAL INTELLIGENCE IN THE DEFENCE SECTOR

Hmyriia Viktoriia^{1[0000-0003-3070-0158]}, **Romanovskaya Lyudmyla**^{1[0009-0002-7284-1493]},
Nikitchenko Anna^{1[0000-0001-9387-5639]}, **Panchenko Anton**^{1[0009-0003-9254-6464]}

State Research Institute for Testing and Certification of Armaments and Military
Equipment, Cherkasy, Ukraine

Abstract. The international experience of recent wars shows that modern warfare is characterised by high intensity and dynamics. This causes significant flows of information, the processing of which and rapid decision-making require considerable effort and time, as a large number of variable factors must be taken into account. Rapid changes in the situation on the battlefield require not only prompt but also proactive response and forecasting of possible scenarios. At the same time, the human factor and the difficulty of making quick and effective decisions can significantly affect the course of hostilities. In such circumstances, the introduction of artificial intelligence algorithms helps to solve complex and potentially dangerous tasks and increases the effectiveness of the use of weapons. Technological innovations combined with artificial intelligence are becoming a key success factor in modern warfare. Therefore, research aimed at their development is extremely important.

Keywords: artificial intelligence, war, cybersecurity, data set, defence.

Вступ. Штучний інтелект (далі - ШІ) все частіше використовується у військовій сфері для підвищення ефективності та точності військових операцій, прогнозного аналізу та логістики. Здатність обробляти великі обсяги даних у реальному часі і навчатися автономно, робить ШІ потужним потенціалом у сфері оборони і національної безпеки.

Однак його використання також піднімає значні етичні та правові проблеми, такі як прозорість у прийнятті рішень і відповідальність у разі помилок або супутньої шкоди.

Деякі цивільні технологічні компанії, зокрема виробники товарів оборонного призначення, беруть активну участь у розробці військового ШІ, хоча існують побоювання, що військові системи ШІ можуть виявитися вразливими до атак і втручання або спричинити випадкову шкоду у великих масштабах. Є також питання щодо відповідальності та прозорості в умовах нинішньої геополітичної нестабільності, особливо якщо врахувати, що США, Китай, росія, Іран,

Туреччина та Ізраїль, серед інших країн, очолюють розробку ІІІ для широкомасштабних військових операцій.

Потенціал ІІІ військового призначення величезний і різноманітний, важливість якого полягає в здатності аналізувати великі обсяги даних із різних джерел, таких як супутникові знімки, сигнали розвідки, засоби зв'язку і соціальні мережі, для виявлення закономірностей і тенденцій, які можуть мати відношення до національної безпеки. Завдяки цій здатності ідентифікація цілей на зображеннях і відеозаписах спостереження надає критично важливу інформацію на полі бою.

Це підводить до використання ІІІ в системах озброєння і автономних транспортних засобах, таких як дрони, наземні транспортні засоби і системи протиповітряної оборони, де втручання людини є мінімальним.

Аналіз літератури та постановка проблеми. Метою даного дослідження є вивчення переваг і викликів використання штучного інтелекту у військових операціях і оборонних системах. Із цією метою сформульовано питання дослідження: Які основні переваги та етичні проблеми пов'язані з інтеграцією можливостей штучного інтелекту у військову сферу? Методологія дослідження полягає в ґрунтовному огляді існуючих наукових досліджень щодо застосування штучного інтелекту у військовому контексті.

Впровадження штучного інтелекту (ІІІ) у військову сферу є предметом численних досліджень як вітчизняних, так і зарубіжних вчених. Ці дослідження охоплюють різні аспекти застосування ІІІ, від еволюції технологій до практичного використання в бойових умовах. У статтях [1,2] досліджено еволюцію ІІІ та проаналізовано бачення щодо розвитку технологій ІІІ. Автори відзначають, що ІІІ проходить швидкий розвиток, і його впровадження у військову сферу може значно підвищити ефективність бойових дій. В іншому дослідженні [3] вивчено досвід Ізраїлю, США з використання ІІІ під час військових дій та у цивільній сфері. Автори підкреслюють, що Ізраїль активно інтегрує ІІІ в свої оборонні системи, що дозволяє швидко аналізувати великі обсяги даних і приймати оперативні рішення на полі бою. Дослідження [4] розглядає особливості застосування ІІІ у сфері військової

логістики. Використання ІІІ в логістичних системах може оптимізувати постачання, зменшити витрати та підвищити оперативність забезпечення військових підрозділів необхідними ресурсами. У роботі [5] відзначено, що фінансове забезпечення впровадження ІІІ та робототехніки військового призначення дозволяють зменшити ризики для життя людей. Це підвищує безпеку військовослужбовців та ефективність виконання бойових завдань. У роботі [6] аналізується використання штучного інтелекту (ІІІ), який приносить значні переваги, але також створює нові загрози в різних галузях, особливо в контексті інформаційної безпеки та кібербезпеки. Автори підкреслюють необхідність розробки заходів для захисту від потенційних загроз, пов'язаних з використанням ІІІ.

Ці дослідження підкреслюють важливість інтеграції ІІІ у військову сферу для підвищення ефективності та безпеки, а також необхідність врахування потенційних ризиків та загроз, пов'язаних з його використанням.

Результати. Штучний інтелект військового призначення відноситься до систем ІІІ, який розроблено і використовується виключно для військових і оборонних застосувань [1]. Даний ІІІ призначено для задоволення суворих вимог і викликів, пов'язаних із військовим середовищем [2], де військові прагнуть отримати вирішальну перевагу над потенційними супротивниками. Наведено характеристики цього типу ІІІ:

- Міцність і надійність. ІІІ розроблений так, щоб працювати надійно і витримувати суворі умови. Він має функціонувати в різноманітних середовищах і умовах, зокрема, в умовах екстремального застосування. Це означає, що необхідно діяти у ворожому середовищі і протистояти фізичним пошкодженням, наприклад, у зоні бойових дій, і зберігати свою функціональність навіть за наявності перешкод або кібератак [3].

- Обчислювальна потужність. ІІІ розроблений з передовими обчислювальними можливостями для забезпечення належної обробки великих обсягів даних. Він може виконувати складні завдання з аналізу та обробки інформації швидко та ефективно. Це означає, що його дизайн і розробка в багатьох випадках є індивідуальними.

- Автономність. Озброєння та військова техніка, а також програмне забезпечення, яке використовується у військових операціях, потребують систем штучного інтелекту, що можуть працювати автономно, без необхідності постійного нагляду з боку людини. Це стосується таких завдань, як навігація безпілотної літачки на полі бою, виявлення і відстеження цілей або управління логістикою і ланцюгами поставок.

- Адаптивність. ШІ дуже легко адаптується і може пристосовуватися до різних ситуацій і мінливих сценаріїв на полі бою.

- Прийняття рішень. Системи штучного інтелекту, в більшості мають приймати рішення в режимі реального часу через мінливу динаміку інформації. Це вимагає вдосконалених алгоритмів і високопродуктивних обчислювальних потужностей.

- Безпека та конфіденційність. З огляду на чутливий характер своїх завдань, системи ШІ військового призначення мають відповідати жорстким стандартам безпеки і конфіденційності. Це включає шифрування, захищені канали зв'язку і заходи для запобігання втручанню або несанкціонованому доступу. Конструкція чіпів має бути стійкою до кібератак, пошкодження даних, збоїв обладнання та інших загроз, оскільки вони будуть використовуватися у військових операціях із високим ступенем ризику.

- Етичні міркування. Системи ШІ повинні бути розроблені таким чином, щоб поважати міжнародне право і мінімізувати ризик заподіяння шкоди цивільному населенню [4].

- Людино-машинна взаємодія: ШІ може працювати автономно або у співпраці з людьми-операторами. Людино-машинна взаємодія має важливе значення у військовому середовищі, де оператори можуть застосовуватися можливості ШІ для обробки та аналізу даних з метою підтримки прийняття обґрунтованих рішень. Ще одна особливість даного типу ШІ полягає в тому, що він зазвичай має доступ до величезних масивів даних для навчання, включаючи військову розвідку, дані спостереження, інформацію з конфліктів і військових ігор, що дозволяє навчатися набагато швидше і досягати вищих рівнів

ефективності. Щоб це стало можливим, необхідні передові технології штучного інтелекту, які виходять за рамки комерційно доступних. Деякі з них розробляються компаніями і військовими підрядниками, що спеціалізуються на ШІ, чії специфічні правила і політика орієнтовані на застосування, пов'язані з обороною і національною безпекою.

Технології, поєднані зі штучним інтелектом, представляють власні розробки та виклики, як, наприклад, у випадку з мікросхемами штучного інтелекту, спеціалізованими для різних функцій у збройних силах і службах безпеки [5, 6]. Наприклад, ШІ для домінування в повітрі та оборони використовує системи технічного зору та машинне навчання для ідентифікації та відстеження цілей. У випадку з автономізацією транспортних засобів зосереджується на навігації, сприйнятті, прийнятті рішень тощо.

На світовому безпековому рівні запроваджено кілька прикладів зброї зі штучним інтелектом, які вже використовуються:

- Harpy - Ізраїльський безпілотно-камікадзе, який використовує ШІ для автономного пошуку і знищення радіолокаційних випромінювачів і систем протиповітряної оборони.

- SGR-A1 - це південнокорейська автоматизована роботизована турельна гармата виробництва Samsung, яка використовує штучний інтелект для виявлення людських цілей і атакує їх вогнепальною зброєю без втручання людини. Вона розгорнута вздовж корейської демілітаризованої зони.

- Sky Warrior/Predator XP - американський безпілотно на базі штучного інтелекту з покращеною автоматизацією та автономністю. Цей безпілотно може здійснювати атаки без нагляду людини. Використовується для цілеспрямованих атак на важливі об'єкти.

- Mantis - це пілотований кулемет зі штучним інтелектом, розроблений американською компанією SparkCognition. Він використовує комп'ютерний зір для автоматичного виявлення та відстеження людських цілей і наведення на них без ручного коригування.

- A10-AJ - це III-модернізація, розроблена компанією Boeing для існуючих штурмовиків A10 Warthog. Він використовує комп'ютерний зір для ідентифікації цілей швидше, ніж людина. Дозволяє пілотам справлятися з більшою кількістю загроз за менший час. Але для запуску зброї має бути людина-оператор.

- Informant V2 - система розпізнавання цілей зі штучним інтелектом, розроблена компанією BAE Systems. Вона покликана допомогти військовим ідентифікувати потенційні загрози та зосередити увагу на тому, що має найбільше значення в бойових ситуаціях.

- LOCUST - система, що складається з рою дронів зі штучним інтелектом, яку розробили в США. Рій дронів може автономно виявляти та ідентифікувати цілі, а потім координувати атаку з мінімальним втручанням людини [21]. Подібні ініціативи розвивають й інші країни.

- XQ-58A Valkyrie - тактичний автономний літак класу «повітря-повітря» і «повітря-земля», який працює з III для проведення різних операцій. Це перший повністю робочий літак шостого покоління.

- Ракети - кілька країн розробляють ракети зі штучним інтелектом, які можуть автономно ідентифікувати і відстежувати рухомі цілі. Включаючи американський рій мікродронів Perdix і китайські ракети DR-8.

- Танки - наддержави досліджують використання III для управління танками з більшою автономією, що включає автоматичне виявлення цілей, навігацію по різних типах місцевості і вибір оптимальних маршрутів.

- Підводні човни - III і автоматизація досліджуються для підводних операцій для вирішення складних завдань, таких як аналіз даних із датчиків, управління бойовими системами і оцінка загроз. Ця технологія має на меті зменшити чисельність необхідного екіпажу і підвищити ступінь автономності.

На сьогодні, існує перший автономний підводний човен, XLUUV (Orca) компанії Boeing, який поєднує в собі ці характеристики.

- Кораблі - безпілотні кораблі зі штучним інтелектом розробляються для таких місій, як розвідка, виявлення мін і атаки. Прикладами цього є кораблі ВМС США Sea Hunter і Sea Hawk, а також норвезький безпілотник Black Hornet.

- Артилерійські системи - деякі артилерійські гармати поєднані зі штучним інтелектом і автоматизацією наведення, що дозволяє їм виявляти, класифікувати і вражати рухомі цілі за лічені секунди, а не хвилини.

- Roadrunner - автономний літальний апарат багаторазового використання з вертикальним зльотом і посадкою (VTOL). Його функція - повітряна і наземна оборона, де він може запускати, ідентифікувати, перехоплювати і знищувати різні типи повітряних загроз. Він використовує кілька систем штучного інтелекту, які дозволяють одному оператору контролювати рої цих БпЛА, створюючи в процесі автономні платформи для спільної роботи.

- Гвинтівки - прототипи снайперських гвинтівок зі штучним інтелектом можуть виявляти людські цілі, розраховувати дальність, напрямок вітру і пропонувати місце для пострілу.

- Cyberglobes - інструмент, який виявляє злочинну діяльність, таку як фінансове шахрайство, торгівля наркотиками, кібератаки та терористичну діяльність в режимі реального часу за допомогою аналізу даних, згенерованих у соціальних мережах і розмовах. Крім того, система має додаткові функції, такі як картографування даних і геолокація [7].

- Небесний щит - сучасна ізраїльська багатоцільова система радіоелектронної боротьби, вбудована в бойові літаки. Розгортає контрзаходи для протидії загрозам, створюючи безпечні коридори для авіаційних ескадрилій з метою оборони та нападу.

- Drone Dome - зенітна система проти безпілотників, яка знищує їх за допомогою електронних перешкод та вдосконаленого штучного інтелекту, що дозволяє швидко виявляти цілі та знищувати їх за допомогою лазерної системи наведення променя.

- Imilite - система, призначена для розвідки, спостереження та рекогносцировки на полі бою, яка інтегрує в собі безліч датчиків і платформ для інтелектуального та ефективного використання. Вона спеціалізується на централізації та уніфікації обробки і використання різних типів даних, таких як зображення і відео, а також інших видів розвідданих.

- MXSERVER - інструмент для аналізу відео- та фотоматеріалів, який використовує розпізнавання облич та машинне навчання, що дозволяє ідентифікувати підозрюваних та надавати корисну інформацію органам безпеки.

- Sea Breaker (морський розбійник) - ракета, що спеціалізується на вибіркових ударах із використанням алгоритмів ШІ та штучного зору.

- Iron Vision - система штучного зору високої чіткості, вбудована в танки, яка дозволяє операторам спостерігати за навколишнім середовищем під кутом 360 градусів. Це дає змогу точніше виявляти цілі за допомогою алгоритмів штучного інтелекту, що забезпечують ситуаційну обізнаність.

- Керована енергетична зброя - складається з точного відстеження повітряних або наземних цілей і знищення їх пострілами лазерного променя за посередництва передового програмного забезпечення зі штучним інтелектом. Існують різні прототипи, що перебувають на стадії розробки і випробувань, наприклад, система 8x8 VBCR північноамериканського сімейства Stryker.

Існує широкий спектр автономних озброєнь і систем, функціональність яких безпосередньо пов'язана зі штучним інтелектом, та наразі перебувають на стадії розробки або мають обмежене оперативне застосування, за винятком таємних досліджень військових і приватних виробників, що не стають надбанням громадськості. Хоча більшість із них все ще потребують людської допомоги для роботи, але наразі спостерігається чітка тенденція до більшої автономності і меншої участі людини.

Наприклад, винищувачі п'ятого і шостого поколінь мають вбудований ШІ для розвідки, виявлення, планування і звичайних, і електронних атак з тривимірним баченням, що усуває пілота від прийняття рішень при наявності безлічі змінних, які можуть збити його з пантелику на полі бою.

Особливістю цієї технології є її масштабованість, тобто її можна оновлювати і включати нові розробки в існуючі, без необхідності починати нові розробки з нуля, як у випадку з інтегрованими військовими системами; звертаючись до відкритих архітектур сенсорних систем, відкритих модульних наборів стандартів C5ISR/EW(CMOSS) і середовищ повітряного базування,

серед іншого, залучаючи такі технології, як передові радіолокаційні системи, авіоніку, навігацію, радіоелектронну боротьбу, розвідку сигналів, зв'язок та інші важливі для виконання місій військові системи.

У військовій промисловості існують різні алгоритми штучного інтелекту, які широко використовуються для різних застосувань:

Штучні нейронні мережі (ШНМ) - це тип алгоритму машинного навчання, створений людським мозком. ШНМ можна використовувати для різних завдань, таких як розпізнавання зображень, обробка природної мови (NPL) і розпізнавання мови. Ці мережі складаються з безлічі взаємопов'язаних штучних нейронів. Кожен нейрон отримує вхідні дані, що обробляються за допомогою набору функцій активації, а потім виробляє обумовлені вихідні дані, доки не буде отримано ідеальний вихідний сигнал.

Машини опорних векторів (SVM) - алгоритм машинного навчання, який можна використовувати для задач класифікації та регресії. SVM працюють, знаходячи гіперплощину, яка розділяє дані на два класи, максимізуючи різницю між класами даних. Навчальні дані відображаються в простір вищої розмірності за допомогою функції ядра, що дозволяє знаходити нелінійні гіперплощини.

Під час навчання вибираються опорні вектори, які є найближчими точками даних до гіперплощини поділу. На етапі класифікації нові дані зіставляються з тим самим високорозмірним простором і відносяться до класу на основі їхнього розташування.

Дерево рішень - це алгоритми керованого навчання, що використовуються для задач класифікації та регресії. Дерево рішень працює шляхом побудови деревоподібної структури, яка представляє взаємозв'язки між певними характеристиками та цільовою змінною. Вони також пов'язані з алгоритмами навчання випадкових «лісів», які поєднують кілька дерев рішень для підвищення точності прогнозування.

Варіаційні автокодери (VAE) - це клас моделей глибокого навчання, які поєднують потужність нейронних мереж з імовірнісними графічними моделями. Вони складаються з двох основних компонентів: кодувальної мережі та

декодувальної мережі, де VAE навчаються на вхідних даних, які можуть бути відібрані, щоб генерувати нові дані, схожі на них. ШНМ може навчитися генерувати нові зображення або дані, подібні до навчальних даних.

Комп'ютерний зір - це галузь ШІ, яка дозволяє машинам інтерпретувати та розуміти візуальні дані з навколишнього світу. Використовується для таких завдань, як виявлення і відстеження об'єктів, розпізнавання облич і автономна навігація.

Обробка природної мови (NLP) - це технологія, яка дозволяє легко і швидко узагальнювати складні тексти. Вона використовує алгоритми для визначення та/або генерування основних ідей та узагальнення їх у короткому тексті, подібно до перекладачів та чат-ботів. Цю технологію можна використовувати в різних галузях, від освіти та журналістики до систем електронного шпигунства.

Когнітивні обчислення - займається створенням інтелектуальних обчислювальних систем, здатних міркувати, навчатися, вирішувати проблеми і приймати рішення без втручання людини. У військовій сфері використовується в обробці зображень, стратегічному плануванні, логістиці та кібербезпеці.

Мультимодальні моделі - може розуміти і обробляти кілька типів даних одночасно, наприклад, текст, зображення, аудіо або мультимодальні комбінації. Цей тип ШІ охоплює раніше згадані моделі, а також інші, які перебувають на стадії розробки, такі як Large Language Models as Optimizers [5], що має на меті покращити продуктивність великих мовних моделей (LLM) шляхом оптимізації за допомогою підказок (OPRO); це не що інше, як метаіндикатори, описані природною мовою, які генерують правдоподібні рішення, засновані на описі проблеми і попередніх рішеннях.

З точки зору прогнозів, ШІ, як очікується, продовжить ставати більш інтегрованим у військове поле. Швидше за все, побачимо більш персоналізований досвід завдяки ШІ, а також вдосконаленню в цивільних галузях, таких як охорона здоров'я, транспорт та освіта. Однак ці досягнення також спричиняють проблеми, особливо щодо таких питань, як конфіденційність та безпека.

Незважаючи на те, що загальні характеристики військового ІІІ схожі на комерційний ІІІ з точки зору машинного навчання, комп'ютерного зору тощо, обсяг, продуктивність, безпека, етика та роль у військових роблять ці системи відмінно від того, що є комерційно доступним. Додамо, що ресурси, виділені для інвестування в цю технологію, значні, і, отже, розширюють межі технології ІІІ, як зазначено.

Експерти [6] стверджують, що люди завжди повинні підтримувати остаточний контроль над будь - якою системою зброї, що включає ІІІ. Інші вважають, що повна автономія неминуча і необхідна для того, щоб не відставати від технологічних досягнень від потенційних загроз [7,8], особливо коли геополітична динаміка сьогодні все більш нестабільна.

Ще один аспект, який слід врахувати, - це потенційне використання військових ІІІ для шпигування цивільних. Хоча шпигунство не є новим, використання ІІІ для цієї мети є новим, особливим, тому ці дії здійснюються не тільки силами безпеки, а й цивільними. Це приклад того, що військові події ІІІ неминуче пробиваються в цивільне життя в різних контекстах, які можуть негативно вплинути на приватне життя, спостереження та інші аспекти повсякденного життя. Нещодавні дослідження [9] виявили, як військовий ІІІ для використання в розвідувальних операціях з метою виявлення терористичних загроз, використовується для моніторингу та спостереження за працівниками, особливо в США.

Мета полягає в тому, щоб здійснити аналіз даних для виявлення організаторів, де виникає можливість страйків праці та діяти проти них. Наприклад, розташування організаторів, щоб їхні роботодавці могли звільнити їх, перш ніж сформувати об'єднання. Ця система може використовуватися роботодавцями під час набору персоналу, щоб уникнути найму майбутніх організаторів профспілки або людей, які мали проблеми в місцях, де вони раніше працювали.

Проблема тут не закінчується, оскільки деякі ІІІ використовуються для виявлення емоцій, які все ще мають недоліки, перевірені упередження, дискримінацію та неправильні припущення. Це означає, що люди можуть бути

помилково звинувачені. В даний час цьому сценарію не вистачає регулювання, а, отже, кілька компаній використовують цей тип технологій без будь-якого контролю або гарантії прозорості. Звідси випливає, що коли ІІІ стає більш інтегрованим у наше життя, питання, пов'язані з етикою та стандартами, стають значущим.

Сюди входять такі проблеми, як конфіденційність даних, можливість алгоритмічного упередженості та вплив ІІІ на робочі місця; вилучення постійних досліджень та розробок у безпеці та дослідженні методів для забезпечення безпечної та надійної реалізації системи ІІІ. Дивлячись у майбутнє, військовий ІІІ має декілька дуже релевантних прогнозів, з потенціалом для покращення, дотримуючись закону про результати роботи Мура [10]. Це передбачає високу обчислювальну потужність та дані, доступні для підготовки моделей ІІІ, що подвоюється приблизно кожні два роки. Тобто, існує безперервний прогрес у поглибленому вивченні, з дослідженням більш складних архітектур, методів оптимізації та стратегій навчання для вирішення ще складніших завдань.

Це просування йде з постійним вдосконаленням невідконтрольного навчання та самодосконаленого навчання [10], що полегшує військовим системам ІІІ вчитися з не маркованих даних та зменшити їх залежність до великих наборів даних. Дані події також привернули увагу до етичної та відповідальної практики ІІІ [11]. Це включає вирішення таких питань, як упередженість, справедливість, прозорість та надійність систем ІІІ. На цьому етапі досліджується інтеграція ІІІ з іншими новими технологіями.

Сюди входять нейротехнологія, нейроморфні обчислення та квантові обчислення. Ці інтеграції передбачають нові можливості для вдосконалення обчислювальної потужності та алгоритмічних можливостей ІІІ. Наприклад, ІІІ має потенціал для революції в діагностиці, лікуванні та наданні медичної допомоги, забезпечуючи взаємодію та безпеку в критичних системах, вдосконалення в цілому охорони здоров'я, виявлення нових препаратів та масштабування персоналізованої медицини на нових рівнях. Незважаючи на те, що технології мають великий потенціал для перетворення багатьох сфер, існують

також етичні проблеми щодо їх використання в корпоративних, суспільних та глобальних військових операціях.

ІІІ при прийнятті автономних рішень може мати наслідки в житті людей. Це тягне за собою встановлення етичної та юридичної бази для її застосування у військовій галузі та чітко визначення відповідальності у випадку помилок або побічних результатів. Майбутні розробки повинні бути збалансовані, з урахуванням конфіденційності, безпеки та прав людини. Таким чином, залежність від ІІІ у військових операціях може бути ризиком, якщо система не застосовується або порушені супротивниками.

На даний момент ІІІ може бути сприйнятливим до упередженості та дискримінації, що викликає негативні наслідки у військових операціях, підриваючи довіру до критичних систем. Важливо також, щоб військові активно вирішили ці виклики та працювали над рішеннями, що дозволять відповідати та ефективно використовувати ІІІ.

Висновки. Військовий ІІІ покликаний задовольнити потреби військових у різних сферах, враховуючи передові можливості переробки, пристосованість та безпеку, серед інших аспектів. Його застосування варіюється від визнання та спостереження до прогностного аналізу для прийняття стратегічних рішень. Основна мета - підвищити ефективність та виконання військових операцій, таких як автономні транспортні засоби (такі як безпілотники або безпілотні підводні човни), кібер -захист, логістика та управління ланцюгами поставок, серед інших.

ІІІ все частіше відіграє вирішальну роль у покращенні захисту кібербезпеки для військових. Автоматизуючи завдання, прискорюючи виявлення та допомагаючи в розвідці загрози, ІІІ Technologies може допомогти військовим більш ефективно захистити свої цифрові активи та критичну інфраструктуру щодо кібератак.

Незважаючи на те, що повністю автономна зброя ще не існує, існує багато прикладів, що покращують наявні системи зброї, забезпечуючи виявлення, пріоритетність, відстеження та цільові рекомендаційні можливості, але остаточне рішення про залучення та використання смертельної зброї все ще наразі потрапляє до оператора людини. Серед різних країн триває гонка військового штучного

інтелекту, який викликає численні актуальні етичні та безпечні міркування, які повинні бути вирішені, коли ця технологія продовжує розвиватися.

Зокрема, значна частина цього технологічного прогресу відбувається поза громадськістю. Слід також визнати, що посилення геополітичної напруженості між великими світовими державами - це прискорення зусиль для розвитку передового ІІІ як для оборони, кібербезпеки, так і для потенційних кібер - можливостей, що ще більше посилює гонку озброєнь у цій галузі.

Отже, оскільки системи ІІІ все більше розгортаються для цілей як кібер - захисту, так і кіберзлочинності, ретельне міжнародне управління та нагляд будуть життєво важливими в майбутньому, щоб допомогти керувати складними етичними наслідками безпеки прогресу в цих технологіях.

Список джерел:

1. Хаустова, В. Є., Решетняк, О. І., Хаустов, М. М., & Зінченко, В. А. (2022). Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. *Бізнес Інформ*, 3, 17–26. <https://doi.org/10.32983/2222-4459-2022-3-17-26>
2. Laudien, T., Ernst, J., Schmerwitz, S. (2023). Bringing a colored head-down display symbology heads up: display fidelity review of a low-cost see-through HMD. *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications*, Vol. 12538, pp. 191–197. DOI: 10.1117/12.2664840.
3. Evron, Y., Bitzinger, R. A. (2023). *The fourth industrial revolution and military-civil fusion: A new paradigm for military innovation?* Cambridge University Press
4. Gaba, S., Budhiraja, I., Kumar, V., Martha, S., Khurmi, J., Singh, A., Singh, K., Askar, S., Abouhawwash, M. (2024). A systematic analysis of enhancing cyber security using deep learning for cyber physical systems. *IEEE*, Vol. 12, pp. 6017–6035. DOI: 10.1109/ACCESS.2023.3349022.
5. Raaijmakers, S. (2019). Artificial intelligence for law enforcement: Challenges and Opportunities. *IEEE Security & Privacy*, Vol. 17, No. 5, pp. 74–77.
6. Maschmeyer, L. (2022). Subverting skynet: the strategic promise of lethal autonomous weapons and the perils of exploitation. *14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, Vol. 700, pp. 155–171. DOI: 10.23919/CyCon55549.2022.9811008.
7. Müller, O., Rotter, S. (2017). Neurotechnology: Current developments and ethical issues. *Frontiers in Systems Neuroscience*, Vol. 11, No. 93, pp. 1–5. DOI: 10.3389/fnsys.2017.00093.
8. Pekarev, J. (2023). Attitudes of military personnel towards unmanned ground vehicles (UGV): a study of in-depth interview. *Discover Artificial Intelligence*, Vol. 3, No. 1, pp. 24. DOI: 10.1007/s44163-023-00058-4.

9. Qian, S., Liu, M., Dou, Y., Fink, Y., Yan, W. (2023). Una ley de Moore para fibras permite tejidos inteligentes. *Revista Nacional de Ciencias*, Vol. 10, No. 1, DOI:10.1093/nsr/nwac202.
10. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. <https://doi.org/10.28925/2663-4023.2023.22.618>
11. Raaijmakers, S. (2019). Artificial intelligence for law enforcement: Challenges and Opportunities. *IEEE Security & Privacy*, Vol. 17, No. 5, pp. 74–77.
12. Rani, V., Nabi, S. T., Kumar, M., Mittal, A., Kumar, K. (2023). Self-supervised learning: A succinct review. *Archives of Computational Methods in Engineering*, Vol. 30, No. 4, pp. 2761–2775. DOI: 10.1007/s11831-023-09884-2.
13. Sattler, S., Pietralla, D. (2022). Public attitudes towards neurotechnology: Findings from two experiments concerning brain stimulation devices (BSDs) and brain-computer interfaces (BCIs). *PloS One*, Vol. 17, No. 11, p. e0275454. DOI: 10.1371/journal.pone.0275454
14. Трофименко, О. Г., & Яремчук, М. В. (2023). Штучний інтелект у військовій сфері. Кіберпростір в умовах війни та глобальних викликів ХХІ століття: теорія та практика: матер. міжнар. наук.-практ. конф., 144–148. <https://doi.org/10.32837/11300.27179>
15. Quirión, R. (2023). Brain organoids: are they for real? *Frontiers in Science*, Vol. 1, p. 1148127. DOI: 10.3389/fsci.2023.1148127.
16. Johnson, J. (2020). Artificial intelligence: A threat to strategic stability. *Strategic studies quarterly*, Vol. 14, No. 1, pp. 16–39.