Юрій ДАНИК, Віталій АНДРЕЙЧУК

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ: МОЖЛИВОСТІ ТА ВИКЛИКИ, ПРОТИДІЯ РИЗИКАМ І ЗАГРОЗАМ

Юрій Даник
Доктор технічних наук, професор,
професор кафедри інформаційної безпеки,
Національний технічний університет України «КПІ»
імені Ігоря Сікорського, Київ

Віталій Андрейчук
Кандидат наук з державного управління,
ст. наук. співробітник,
Міжнародний науково-навчальний центр інформаційних
технологій та систем Національної академії наук України
та Міністерства освіти та науки України, Київ

Анотація

У статті досліджується роль штучного інтелекту у сфері національної безпеки та оборони. Розкриваються можливості, виклики, ризики та загрози, пов'язані з використанням штучного інтелекту. Аналізуються партнерство та конкуренція, технологічні та геополітичні наслідки розвитку штучного інтелекту, зокрема в контексті сучасного етапу міжнародних відносин. Розглядаються етичні та правові аспекти, такі як проблеми безпеки і конфіденційності даних, а також відповідальність за автономні системи. Авторами запропонована обґрунтована система заходів для розвитку та забезпечення штучного інтелекту у сфері національної безпеки і оборони. Стаття висвітлює важливі аспекти, які варто враховувати при розробці стратегій використання штучного інтелекту для національної безпеки і оборони та їх практичної реалізації.

Ключові слова: *штучний інтелект, національна безпека, оборона, етика, безпека даних, автономні системи, геополітика, кадровий потенціал, кіберзахист, міжнародна співпраця.*

ARTIFICIAL INTELLIGENCE IN NATIONAL SECURITY AND DEFENSE: OPPORTUNITIES AND CHALLENGES, RISK AND THREAT MITIGATION

Yuriy Danyk
Doctor of Technical Sciences, Professor,
Professor of the Department of Information Security,
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv

Vitalii Andreichuk
Candidate of Sciences in Public Administration,
Senior Scientist,
International Research and Training Center of Information Technologies
and Systems of the National Academy of Sciences of Ukraine
and the Ministry of Education and Science of Ukraine, Kyiv

Abstract

This article explores the role of artificial intelligence in the field of national security and defense. It reveals the opportunities, challenges, risks, and threats associated with the use of artificial intelligence. The article analyzes partnerships and competition, technological and geopolitical consequences of artificial intelligence development, particularly in the context of the current stage of international relations. Ethical and legal aspects are considered, such as data security and privacy issues, as well as responsibility for autonomous systems. The authors propose a substantiated system of measures for the development and provision of artificial intelligence in the field of national security and defense. The article highlights important aspects to consider when developing strategies for the use of artificial intelligence for national security and defense and their practical implementation.

Keywords*: artificial intelligence, national security, defense, ethics, data security, autonomous systems, geopolitics, human resources, cybersecurity, international cooperation.*

Вступ

Ідеї щодо створення штучних об'єктів, подібних людині, машин, які можуть думати, бачити, сприймати оточуючий світ, розуміти людську мову та свідомо діяти для досягнення певних результатів, з'явилися у людей ще декілька тисяч років тому. Наприклад, у давньогрецькому міфі про Талоса — броньованого велетня, який оживав під впливом магічних променів. У працях письменників-фантастів опис того, що пізніше отримало визначення штучного інтелекту (ШІ), з'являється в 19 столітті. У 1863 році англійський письменник Семюел Батлер написав листа редактору газети з новозеландського Крайстчерча. У цьому листі, під назвою «Дарвін серед машин», висловлювалася ідея «живого механізму», який колись зможе так розвинутися, що зрівняється

з людьми, а може, навіть перевершить їх. Автор закликав до боротьби проти появи таких механічних істот і заявляв, що «машини подібного роду мають бути знищені» [1].

Загальнотеоретичні, математичні та логічні основи створення штучного інтелекту почали формуватися в багатьох країнах світу в 40–50-х роках минулого століття. Вони знайшли своє відображення в працях Вілкеса[2], Вінера[3], Семуеля[4], Неймана[5], Марвіна Мінскі, Натаеля Рочестера і Клода Шеннона[6]. Алан Тьюрінг, який є одним із засновників теорії скінчених автоматів і автором тесту для перевірки, чи є комп'ютер розумним у людському сенсі слова, який він опублікував у 1950 році в статті «Обчислювальні машини та розум», вважається одним із перших засновників теорії штучного інтелекту[7].

Словосполучення «штучний інтелект» запропонував у 1956 році викладач математики Дартмутського коледжу Джон Маккарті під час конференції, на якій розглядалося, як навчити машини працювати з лінгвістичними текстами, формувати абстрактні поняття та концепції, вирішувати завдання, які вирішують люди та вдосконалюватися. Український вчений академік В. М. Глушков також вніс значний вклад в розробку теорії і практику застосування штучного інтелекту[8].

У 70–80 роках 20 століття розвиток знань щодо штучного інтелекту отримав більш конкретний і прикладний обрис[9],[10]. Вводяться у вжиток та досліджуються такі складові та механізми штучного інтелекту, як машинне навчання, природні мови, експертні системи, розподілені системи для розв'язання складних завдань, які не можуть бути вирішені за допомогою однієї системи штучного інтелекту та багато іншого. Розвитку також набули

---

[1] Martin Ford. Rise of the Robots: Technology and the Threat of a Jobless Future, New York, Basic Books, 2015, 315 p.

[2] Preparation of Programs for an Electronic Digital Computer (1951), M. V. Wilkes with D. J. Wheeler and S. Gill, Addison Wesley Press

[3] Cybernetics: Or Control and Communication in the Animal and the Machine. Paris, (Hermann & Cie) & Camb. Mass. (MIT Press) ISBN 978-0-262-73009-9; 1948, 2nd revised ed. 1961

[4] A. L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," in IBM Journal of Research and Development, vol. 3, no. 3, pp. 210–229, July 1959, DOI: 10.1147/rd.33.0210.

[5] The Computer and the Brain" by John von Neumann, New Haven, Yale University Press, 1958, 86 p.

[6] A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955 John McCarthy, Marvin L. Minsky, Nathaniel Rochester, Claude E. Shannon, DOI: https://doi.org/10.1609/aimag.v27i4.1904

[7] Alan Turing and others. The Mind and the Computing Machine, The Rutherford Journal, 1950, https://www.rutherfordjournal.org/article010111.html

[8] Синтез цифровых автоматов В. М. Глушков, М. Физматгиз, 1962, 476 с.

[9] Knowledge-based Systems in Artificial Intelligence by Edward A. Feigenbaum and Joshua Lederberg, 1979

[10] Structured Knowledge: A Topographical Approach by Peter Jackson, 1985.

практичні питання створення штучного інтелекту, такі як програмування, моделювання та реалізація складних систем.

Вже тоді визначилися перспективи розвитку і створення інтелектуальних систем, здатних до самостійного навчання на основі даних, самостійного розв'язання завдань та особливості їх застосування в багатьох галузях, таких як медицина, фінанси, транспорт і т.д. (довідник Бортко по штучному інтелекту[11]). Таким чином, в середині 80-х років були розроблені ключові підходи до штучного інтелекту, які стали основою для його подальшого розвитку, зберігаючи свою актуальність й донині. Загалом, історія розвитку штучного інтелекту в 40–80-х роках минулого століття досить детально відображена в довіднику Барра і Фейгенбаума[12].

Поява на початку 21-го століття теорії та практики створення нейромереж і розробка технологій глибокого навчання та інших методів машинного навчання стали важливими моментами у розвитку штучного інтелекту[13, 14, 15, 16, 17]. За даними Всесвітньої організації інтелектуальної власності, від 1998 до 2017 року у США було подано приблизно 50 000 патентних заявок на штучний інтелект, а в Китаї — близько 41 000. На саміті Мадриді в жовтні 2021 року 17 країн-членів НАТО підписали угоду про створення інноваційного фонду розвитку технологій штучного інтелекту на 1 млрд євро.

Військові по всьому світу вкладають значні кошти в дослідження та розробку автономної зброї зі штучним інтелектом. Тільки США у період з 2016 по 2020 роки виділили 18 мільярдів доларів на створення та розвиток автономної зброї[18]. Командування підрозділу Сухопутних військ США, відповідальне за технологічне забезпечення та модернізацію військ (Army Futures Command (AFC)), провело аналіз сфер застосування штучного інтелекту і вибрало 11 найбільш перспективних напрямків для проведення серйозних досліджень у найближчі п'ять років. Особливий інтерес викликає розробка штучного інтелекту для автономних наземних і повітряних платформ, здатних працювати в різних середовищах, включаючи відкриті, міські та ускладнені умови.

---

[11] Бортко Є. Н. Довідник з штучного інтелекту. — М.: Радіо і связь, 1985. — 416 с.

[12] The Handbook of Artificial Intelligence: Volume 1 Paperback — 1 Jan. 1981. English edition by Avron Barr (Autor), Edward A. Feigenbaum (Mitwirkende).

[13] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444.

[14] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[15] Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85–117.

[16] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255–260.

[17] Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., ... & Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 484–489.

[18] Artifcial Intelligence Index Report 2023, Stanford Institute for Human-Centered Artifcial Intelligence, 2023, 385 p.

Німеччина, яка має найбільший сектор досліджень штучного інтелекту в ЄС, оновила свою національну стратегію штучного інтелекту в грудні 2020 року. Вона оголосила про збільшення інвестицій у цей сектор з 2,4 млрд доларів США до 5,9 млрд доларів США до 2025 року.

Британія планує стати наддержавою в галузі штучного інтелекту протягом 10 років. У вересні 2021 року британський уряд завершив розробку плану, який передбачає випередження США і Китаю в сфері штучного інтелекту. Документ «Національна стратегія розвитку штучного інтелекту» має на меті просування використання штучного інтелекту в бізнесі, залучення міжнародних інвестицій в британські компанії в цій галузі та формування нового покоління британських талантів в технологічній сфері. Основна увага приділяється розв'язанню питань національної безпеки і оборони.

У сфері розвитку ШІ все більше задіюються високотехнологічні досягнення з різних галузей науки і техніки. З аналізу досягнень і напрямків розвитку технологій можна прогнозувати використання не лише електронних, але й квантових, біо- та інших комп'ютерів, а також їх комбінацій як базових елементів для реалізації ШІ. Це дозволить значно збільшити швидкість обчислень та вирішити завдання, які не можуть бути повністю розв'язані на класичних комп'ютерах.

Одним з важливих напрямів стало створення багатоагентних систем ШІ, в яких багато агентів взаємодіють між собою та з навколишнім середовищем для досягнення певних цілей. Це може включати розробку систем контролю та управління, мережевих технологій тощо.

З розвитком штучного інтелекту з'явилися нові етичні, соціальні і безпекові проблеми, пов'язані з його використанням, поряд з новими можливостями. Одне з актуальних питань полягає в тому, як забезпечити, щоб штучний інтелект не дискримінував людей за расовими, гендерними, етнічними, соціальними ознаками та іншими факторами, не поширював хибну інформацію, не вводив в оману, залишався під контролем, не створював загроз та був безпечним.

Питання прозорості та обліковості прийнятих рішень, а також відповідальності за можливі негативні наслідки від використання штучного інтелекту, і нормативно-правового регулювання створення, розвитку та використання продуктів ШІ в різних сферах життєдіяльності людини і суспільства є надзвичайно важливими безпосередньо повязані з управлінням ризиками в цій сфері.

В провідних країнах світу вже проводиться інтенсивна робота щодо нормативно-правового регулювання використання технологій у сфері штучного інтелекту[19]. Наприклад, регламент ЄС «Proposal for a Regulation laying

[19] Цяпа С. М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах / С. М. Цяпа // Інформація і право, 2021, № 2 (37). С. 51–59.

down harmonised rules on artificial intelligence» передбачає усунення можливих ризиків та забезпечення прозорого використання штучного інтелекту з обов'язковим дотриманням прав та демократичних цінностей[20]. У цьому регламенті визначено чотири категорії ризику використання штучного інтелекту, проте він не застосовується до військових цілей.

Проте, існують невирішені протиріччя між швидким розвитком ШІ та його використанням, особливо в сфері безпеки і оборони, і необхідністю передбачати виклики, ризики і загрози, пов'язані з його розвитком. Наразі відсутні обґрунтовані системні підходи до зниження, запобігання і нейтралізації цих загроз.

Метою нашого дослідження є аналіз і прогнозування можливостей, які надає штучний інтелект для національної безпеки і оборони, а також викликів, ризиків і загроз, пов'язаних з його розвитком. Ми також пропонуємо заходи щодо їх запобігання та нейтралізації, одночасно сприяючи всебічному розвитку штучного інтелекту.

Основні напрями розвитку і досліджень ШІ

Проведений системний аналіз розвитку та використання продуктів штучного інтелекту показав, що теоретичні розробки і практика їх застосування в різних сферах відбуваються за різними технологічними напрямами, які в різній мірі задіяні при вирішенні конкретних прикладних задач.

Технологічні напрями штучного інтелекту системно включають і поєднують такі складові:

- Представлення знань (Knowledge representation)
- Машинне навчання (Machine learning)
- Візуалізація (Visualization)
- Обробка «природною» мовою (Natural language processing)
- Глибоке навчання (Deep learning)
- Генерування природньої мови (Natural language generation)
- Глибокі системи запитань і відповідей (Deep Q&A systems)
- Віртуальні особисті помічники (Virtual personal assistants)
- Графічний аналіз (Graph analysis)
- Аналіз соціальних мереж (Social network analysis)
- Датчики/Інтернет речей (Sensors/internet of things)
- Робототехніка (Robotics)
- Рекомендаційні системи (Recommender systems)
- Імітаційне моделювання (Simulation modelling)

[20] Proposal for a Regulation laying down harmonised rules on artificial intelligence, 2021. https://ec.europa.eu/newsroom/dae/redirection/document/7578

– «М'яка» робототехніка (Soft robotics)
– Аналіз аудіомовлення (Audio/speech analytics)
– Аналітика зображень (Image analytics)
– Машинний переклад (Machine translation)

Проведений аналіз дозволяє виділити основні напрями розвитку і досліджень штучного інтелекту, які одночасно є і самостійними, і взаємопов'язаними. Ці напрями мають подвійне застосування як на поточний момент, так і в стратегічній перспективі, тому вони потребують окремого розгляду в цьому дослідженні.

Автономні платформи — цей напрямок спрямований на створення безпілотних бойових і транспортних засобів, а також роботів, які можуть самостійно приймати рішення та взаємодіяти з навколишнім середовищем. У цьому напрямку провідними є компанії, такі як IAI, Нортроп Грумман, Arduino, Anduril, Tesla, Waymo та Uber.

Ройові системи — цей напрямок орієнтований на створення безпілотних засобів та роботів, які можуть самостійно приймати рішення та взаємодіяти з навколишнім середовищем, а також між собою, для здійснення спільних дій та вирішення задач у взаємодії.

Машинне навчання — цей напрямок орієнтований на створення алгоритмів, які можуть самостійно навчатися та покращувати свою ефективність з кожним новим досвідом. У цьому напрямку провідні компанії, такі як Google, Facebook та Amazon.

Глибоке навчання та нейромережі — розвиток алгоритмів та моделей для аналізу та обробки великих обсягів даних з використанням нейромереж і глибокого навчання дозволяє створювати більш точні та складні моделі для розв'язання різних задач.

Візуалізація даних та синтетичне середовище — цей напрямок орієнтований на розробку інструментів для отримання, візуалізації, аналізу та обробки великих обсягів даних. Він також включає створення синтетичних середовищ для тестування різних алгоритмів та моделей, поліпшення процесу навчання, віртуальної валідації концепцій і прототипів. У цьому напрямку провідні компанії, такі як Tableau, Qlik та Unity.

Формування віртуального середовища ШІ: Цей напрямок спрямований на створення взаємодіючих віртуальних агентів та середовищ, які можуть взаємодіяти з людиною та навколишнім світом. Провідними компаніями в цьому напрямку є Microsoft, IBM та Amazon.

Відстеження положення, навігація і хронометраж (PNT): Цей напрямок спрямований на точне визначення положення, напрямку та часу. Розробляються методи, алгоритми і можливості злиття та спільної обробки даних з різних джерел для навігації та управління засобами, включаючи умови

блокування традиційних навігаційних систем. Це особливо важливо для автономних транспортних засобів, дронів та інших систем, які потребують точної навігації. Провідними компаніями в цьому напрямку є Trimble, Garmin, Novatel та Honeywell.

Зондування і розпізнавання: Цей напрямок включає розробку систем, які здійснюють виявлення, ідентифікацію та розпізнавання об'єктів, включаючи малоконтрастні та замасковані об'єкти. Використовуються різні типи сенсорів, такі як камери, радари, сонари, лідари і т.ін., а також методи розпізнавання на основі фізичних, поведінкових, цифрових, кібернетичних та інших показників. Застосовується в різних галузях, включаючи автомобільну промисловість, медицину, розвідку, безпеку, транспорт, робототехніку та інші. Проект Maven, що здійснювався за замовленням Пентагону, використовував штучний інтелект для виявлення та відстеження активності противника з відеоканалів. Головний стратегічний директор Anduril Industries (Каліфорнія) Кріс Броуз вважає, що «Справжня цінність штучного інтелекту — це збір та інтеграція даних, що надходять від великої кількості датчиків, та усунення неважливої інформації для військових операторів».

Комунікації і мережі: Цей напрямок включає розробку надійних і безпечних мереж і систем комунікацій між комп'ютерами та пристроями, такими як телефони, планшети, ноутбуки і т.д., а також забезпечення їх сумісності. Системи можуть бути дротовими або бездротовими і використовувати різні протоколи і технології, такі як Bluetooth, Wi-Fi, LTE, 5G і т.д. Застосовується в різних галузях, включаючи транспорт, медицину, військову техніку, телекомунікації та інші.

Обчислення: Цей напрямок включає розробку алгоритмів і систем, які дозволяють здійснювати обчислення з високою пропускною і обчислювальною здатністю та енергоефективністю. Системи можуть використовуватися для обчислення складних математичних формул, розробки нових алгоритмів, обробки великих обсягів даних і т.д. Застосовується в різних галузях, включаючи фінанси, науку, інженерію, медицину, транспорт та інші.

Інтернет речей: Це один із основних напрямів розвитку ШІ, який передбачає взаємозв'язок між фізичними пристроями та програмними рішеннями. Цей напрям включає використання датчиків, пристроїв збору даних, розумних пристроїв та інших засобів для збирання, обробки та аналізу великих обсягів даних з метою автоматизації та оптимізації процесів.

Захист об'єктів та людей: ШІ використовується для виявлення застосування та впливу засобів масового ураження і забезпечення захисту від них. Особлива увага приділяється захисту від кібератак, які є однією з основних проблем у галузі ШІ. За допомогою ШІ розробляються системи захисту, які здатні розпізнавати та нейтралізувати кібератаки.

Підвищення працездатності людини: ШІ використовується для розробки систем, які підвищують працездатність людини, поліпшують її фізичні та психологічні можливості, а також для навчання людей.

Автоматизація аналітики даних: ШІ дозволяє автоматизувати процес аналізу та обробки великих обсягів даних, що призводить до покращення ефективності та швидкості роботи з даними.

Моделювання процесів і систем: ШІ дозволяє моделювати поведінку та передбачати розвиток складних систем, що допомагає розробляти більш ефективні та оптимальні рішення.

Інтеграція систем різних рівнів і поколінь: ШІ використовується для інтеграції різних систем різних рівнів та поколінь з метою забезпечення ефективної спільної роботи і зменшення ризиків виникнення помилок.

Розвиток технологій без участі людини: ШІ використовує машинне навчання, глибинне навчання та інші інструменти для автоматизації процесів та вирішення завдань без прямої участі людини. Це охоплює розробку програмного забезпечення, робототехніку та автономні системи.

Планування та управління логістикою: ШІ використовується для поліпшення ефективності транспортування товарів, управління складними логістичними потоками та зменшення ризиків помилок в процесі виконання.

Розробка інтерфейсів та взаємодія з ШІ: ШІ сприяє розробці нових методів та технологій для зручної та ефективної взаємодії з системами ШІ.

Це лише огляд деяких напрямків розвитку та досліджень в галузі ШІ. ШІ є однією з найбільш динамічних галузей знань, яка постійно генерує нові відкриття та досягнення[21,22].

Застосування ШІ в сфері національної безпеки і оборони

Особливістю сучасних збройних конфліктів є безпосередня і постійно зростаюча високотехнологічність. Відбувається змагання в галузі технологій розробки (R&D) та виробництва, охоплюючи весь спектр засобів і систем, що застосовуються у протиборстві, включаючи технології підготовки та ведення дій, логістики, розвідування, кіберінформаційного забезпечення, захисту особового складу, озброєння та військової техніки.

Успішне забезпечення національної безпеки і оборони, а також всебічний позитивний розвиток суспільства надто залежать від стрімкого розвитку високотехнологічних інновацій. До них відносяться такі напрями, як мехатроніка, роботизовані комплекси, кіберфізичні системи, інформаційні

[21] Artificial intelligence: threats and opportunities. https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities

[22] Opportunities of Artificial Intelligence. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf

технології, кібербезпека, технічна розвідка, радіоелектронна боротьба, криптографія, космічні системи, автоматизовані системи управління, телекомунікаційні системи, енергозабезпечення, квантові, нано- і біотехнології військового призначення. Важливе місце серед цих напрямів займає штучний інтелект.

Штучний інтелект застосовується в сфері безпеки і оборони як для збору та обробки розвідувальних даних, так і для управління застосуванням озброєння та військової техніки. Основною метою впровадження та розвитку штучного інтелекту в цій сфері є досягнення переваги над потенційним противником, уникнення ризиків деструктивних дій з його боку та отримання переваги на полі бою.

Завдяки штучному інтелекту можливе автоматичне збирання, обробка, аналіз та об'єднання даних з різних джерел у реальному часі. Враховуючи моніторинг зон ведення дій, активність противника, інформацію про власні сили та сили противника, комунікаційні системи, озброєння, військову техніку, живу силу противника, метеорологічні та географічні дані, стан місцевості тощо, штучний інтелект може моделювати та прогнозувати розвиток подій та дій противника. Армія США вже експериментально використовує систему на основі штучного інтелекту під назвою «Прометей», яка оцінює діяльність противника на основі зображень у реальному часі, самостійно визначає пріоритетні цілі та видає цілевказівки для автоматичного націлювання засобів ураження. Застосування штучного інтелекту дозволяє автоматизувати процеси прийняття рішень, генерувати варіанти дій з урахуванням ризиків та забезпечує підвищену точність та швидкість реакції на змінні умови та специфіку бойових дій, а також зниження людських втрат.

Системи штучного інтелекту здатні швидко навчатися на основі обробки великих обсягів даних та інформації. Застосування штучного інтелекту в галузі оборони включає не тільки отримання та аналіз інформації про стан театру військових дій, але й кіберзахист, логістику, автономне використання роботизованих засобів тощо. Роботизація озброєння та військової техніки є одним з найперспективніших напрямків розвитку у військовій сфері, і вона стала визначальною ознакою сучасного воєнного конфлікту.

У сфері управління застосуванням озброєння та військової техніки, штучний інтелект (ШІ) може забезпечити автоматичне управління бойовими машинами з можливістю самостійного прийняття і реалізації рішень щодо ураження противника на випередження, з урахуванням ієрархії цілей за рівнем вагомості. Автономні системи озброєння зі штучним інтелектом можуть виявляти і вистежувати майже будь-які цілі, вирішуючи самостійно, коли і як здійснювати вплив на них. Вони мають перспективу отримати здатність відстежувати цілі, що відрізняються за зовнішнім виглядом або поведінкою, навіть без попередніх даних про ці особливості. Вони також

зможуть змінювати цілі та орієнтуватися на незнайомій місцевості в будь-який час доби та за будь-якої погоди, одночасно розпізнаючи та уникаючи дружніх військ і цивільного населення. Масове використання невеликих автономних роботів, які не потребують створення додаткового середовища або інфраструктури для своїх дій, надає величезну перевагу стороні, яка їх застосовує, практично у будь-якому виді конфлікту чи бойових дій. Однак, їх практичне ройове застосування з врахуванням контролю заданої території, виявлення та аналізу практично будь-якої діяльності противника, потребує взаємодії, організації і координації спільних дій сукупності систем ШІ всіх задіяних автономних засобів. Іншими словами, необхідна системна мережева інтеграція вищого рівня.

Тому багато провідних виробників озброєння світового рівня працюють над розвитком систем управління силами і засобами (військами і зброєю), включаючи створення систем управління роями роботів. Лідерами у цій галузі є компанія Нортроп Грумман, яка працює над штучним інтелектом для управління військовими силами, а також такі провідні компанії, як Lockheed Martin та Boeing, які активно впроваджують інноваційні рішення зі штучного інтелекту для підвищення ефективності управління військовими силами та зброєю.

Інтеграція технології штучного інтелекту в системи озброєнь дозволяє зробити їх меншими і дешевшими, здатними швидше реагувати і точніше вражати цілі.

В Україні в даний час активно відбувається розробка, розвиток і впровадження інноваційних форм, способів, методів і тактики ведення сучасних бойових дій, підходів до розробки і планування місій (операцій, акцій) з використанням роботизованих систем, а також впровадження та застосування всього спектру інноваційних високотехнологічних засобів (систем, комплексів), пов'язаних з цими процесами.

Все це вимагає професійних системних і комплексних підходів до збору, вивчення та узагальнення результатів застосування роботизованих засобів (систем, комплексів), отриманого бойового досвіду, розробки обґрунтованих рішень щодо формування та оснащення нових військових підрозділів і структур Збройних Сил, які призначені для ефективного ведення бойових дій з використанням інноваційних високотехнологічних засобів, а також об'єднання їх у відношенні до кіберінформаційного простору (роботизовані системи (комплекси, засоби) наземного, повітряного, надводного (підводного) базування та інші кіберфізичні об'єкти, системи управління типу C4ISR, засоби (сенсори) технічних видів розвідки тощо).

Проте, існують ризики і проблеми, пов'язані з хаотичністю і турбулентністю впровадження інновацій та їх застосування, розробкою і створенням підсистем розвідувально-інформаційного забезпечення бойового застосування

роботизованих комплексів, єдиного системного моделювання та планування місій (операцій), управління застосуванням роботизованих комплексів та інших високотехнологічних засобів за єдиним замислом і планом з раціональною адаптацією до змін обстановки, перспективної моделі структури і архітектури побудови та управління системою роботизації оборони.

Системність у цих процесах є надзвичайно важливою і може значно збільшити їх ефективність і результативність, зменшити кількість помилкових рішень і фінансових витрат, дозволити визначити вірні пріоритети, послідовність дій, порядок оснащення і застосування інноваційних підрозділів і структур, раціонально забезпечити роботизацію оборони в цілому.

Отже, розробка та впровадження систем управління роями роботів, які базуються на штучному інтелекті та мережевій інтеграції, відіграють важливу роль у сучасних військових та оборонних стратегіях. Вони дозволяють покращити ефективність управління військовими силами, забезпечують більш точне та швидше прийняття рішень, підвищують безпеку та знижують витрати. Проте, при їх впровадженні необхідно враховувати системні аспекти, організацію взаємодії різних систем і структур, а також вирішувати етичні й безпекові питання, щоб забезпечити максимальну результативність і безпеку використання штучного інтелекту в військовій сфері.

Проблема наукових досліджень та підготовки фахівців

Ефективне використання штучного інтелекту в сфері національної безпеки і оборони потребує наявності кваліфікованих фахівців. Тому, для забезпечення успішного використання ШІ в цих сферах, окрім формування та розвитку дієвої системи фундаментальних і прикладних наукових досліджень, необхідно створити і розвивати інноваційну інтегровану систему освіти та підготовки фахівців зі штучного інтелекту та високих оборонних технологій загалом для сфери національної безпеки і оборони.

Для досягнення цієї мети потрібно розробити сучасні державні та галузеві освітні стандарти, спеціалізовані програми навчання та підготовки, які спрямовані на формування знань і навичок зі штучного інтелекту та його використання, кібербезпеки, аналізу даних та використання новітніх технологій. Розширення співпраці між університетами, науковими установами та військовими організаціями допоможе створити ефективну систему підготовки фахівців, які зможуть ефективно використовувати штучний інтелект в інтересах національної безпеки і оборони.

Створення спеціалізованих програм досліджень в сфері штучного інтелекту сприятиме розвитку інновацій. Ці програми можуть охоплювати широкий спектр тем, включаючи розробку нових алгоритмів машинного навчання, аналіз даних, кібербезпеку та використання штучного інтелекту для передбачення та прогнозування кризових ситуацій та їх подолання.

Інші важливі сфери застосування ШІ

У сфері публічного управління і державної служби використання ШІ може покращити ефективність обробки даних та прийняття обґрунтованих рішень. Основні напрямки застосування ШІ в цій сфері включають аналіз великих обсягів даних, автоматизацію процесів публічного управління та поліпшення комунікації між урядовими органами та громадянами[23].

У сфері транспорту застосування ШІ призводить до покращення безпеки, ефективності, комфорту та сталості транспортних систем. Основні напрямки включають розвиток автономних транспортних засобів, оптимізацію транспортних мереж та управління рухом, а також покращення систем управління громадським транспортом, оптимізації логістичних мереж при їх проектуванні та здійсненні перевезень.

У сфері телекомунікацій застосування ШІ спрямоване на покращення ефективності, надійності та якості послуг зв'язку. Основні застосування включають оптимізацію мереж, аналітику трафіку, управління якістю обслуговування, персоналізацію послуг та автоматизацію мережевих операцій.

У сфері аграрного виробництва застосування ШІ відкриває широкі можливості для покращення продуктивності, ефективності та стійкості виробництва. Основні напрямки включають аналітику даних, управління роботами, прогнозування погоди, управління ресурсами та системи моніторингу.

У промисловому виробництві застосування ШІ дозволяє автоматизувати та оптимізувати виробничі процеси. Основні застосування включають автоматизацію виробничих ліній, прогнозування та попередження поломок, оптимізацію виробничих процесів та контроль якості.

У медицині штучний інтелект використовується для покращення діагностики, лікування, профілактики захворювань та розробки нових ліків та технологій.

Концепція створення розумних міст та будівель включає застосування ШІ для управління інфраструктурою з метою підвищення комфорту, ефективності використання ресурсів, енергоефективності та раціонального енергозабезпечення[24,25].

У сфері управління інтегральними системами застосування ШІ забезпечує оптимальне керування процесами виробництва, моніторинг стану обладнання, планування та підвищення рівня безпеки на виробництві, а також зниження витрат. Системи автоматизованого керування з ШІ можуть

[23] UN E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

[24] Artificial Intelligence and National Security. https://sgp.fas.org/crs/natsec/R45178.pdf

[25] AI and National Security: Major Power Perspectives and Challenges. https://www.idsa.in/issuebrief/ai-and-national-security-ssharma-120922

прогнозувати потребу в матеріалах та ресурсах, розподіляти завдання між робочими машинами та пристроями, забезпечувати оптимальні параметри роботи техніки та виробничого середовища.

Виклики, ризики та загрози ШІ

Розвиток та застосування штучного інтелекту (ШІ) мають не лише позитивні аспекти, але й потенційні загрози та високі ризики.

Розглядаються ризики, пов'язані з впровадженням ШІ, які виникають через недостатність знань та досвіду, а також ризики, пов'язані з використанням систем штучного інтелекту як складових безпеки продуктів чи систем. Деякі системи ШІ можуть бути віднесені до «високого ризику», оскільки представляють значний потенціал для небезпеки здоров'ю, безпеці та основним правам людини.

У регламенті ЄС Proposal for a Regulation laying down harmonised rules on artificial intelligence пропонуються підходи до класифікації систем ШІ як систем високого ризику, заборони їх використання та визначення інцидентів, пов'язаних з їхнім використанням.

«Серйозним інцидентом», пов'язаним з ШІ, є будь-який інцидент, що може призвести до смерті людини, серйозних травм для здоров'я, збитків майну або навколишнього середовища, або серйозного та незворотного порушення управління та експлуатації критичної інфраструктури.

Регламент також пропонує заборонити використання підсвідомих методів ШІ, які можуть спотворювати поведінку людини та завдати їй фізичну або психологічну шкоду, використання систем ШІ для оцінки благонадійності фізичних осіб державними органами, а також використання систем віддаленої біометричної ідентифікації в загальнодоступних місцях з метою забезпечення правопорядку, крім випадків, коли таке використання є суворо необхідним.

Системи штучного інтелекту вважаються системами високого ризику, якщо вони призначені для використання як компонент безпеки продукту або являють собою самостійний продукт, на який поширюється законодавство ЄС. Такі системи, як і продукти, які включають компонент безпеки ШІ, повинні пройти оцінку відповідності третьою стороною перед введенням їх на ринок або в експлуатацію, оскільки вони представляють ризик для здоров'я, безпеки та основних прав людини.

У системі викликів, ризиків та загроз ШІ можна виділити такі аспекти:

- Використання ШІ як інструменту злочинцями або іншими особами для нанесення шкоди людям або об'єктам.
- Можливість деструктивного впливу людини на ШІ.
- Протиборство між різними системами ШІ.
- Непідконтрольні дії ШІ, які можуть викликати проблеми.

Крім цього, вивчення ШІ показує, що до основних викликів та загроз, пов'язаних з ШІ, належить: зміна балансу сил між державами та іншими акторами через впровадження ШІ. Країни з більшим доступом до технологій штучного інтелекту можуть мати перевагу не лише в економічній та військовій сферах, а й у реалізації своїх потреб та інтересів, що може призвести до нестабільності та конфліктів.

Використання ШІ недержавними суб'єктами, такими як терористичні групи чи злочинні організації, а також звичайними недержавними організаціями, громадськими об'єднаннями і громадянами, може порушити баланс сил між державними та недержавними суб'єктами.

Негативними наслідками є також можливість порушення соціальних систем, включаючи збільшення безробіття, заміщення людей роботами у різних професіях, необхідність перепрофілювання та зростання нерівності.

Також формується та посилюється надмірна залежність людини від штучного інтелекту та інших високих технологій.

Використання людьми з раннього віку деяких можливостей, які надає ШІ, може негативно вплинути на їх когнітивний розвиток, порушити його та призвести до формування залежності від ШІ, відсутності навичок критичного мислення та інших проблем.

Швидкий і неконтрольований розвиток штучного інтелекту може призвести до непередбачуваних наслідків і відсутності відповідальності для тих, хто розробляє та впроваджує системи штучного інтелекту.

Використання штучного інтелекту з високою ймовірністю може призвести до порушення конфіденційності інформації, зокрема особистих даних, комерційної та державної таємниці.

Нерівний доступ до технологій та знань ШІ може призвести до формування технологічного розриву та збільшення нерівності між націями та людьми.

Злочинці все більше можуть використовувати штучний інтелект для здійснення різних незаконних дій, включаючи кіберзлочинність, шахрайство та крадіжку особистих даних.

Неконтрольований розвиток штучного інтелекту може призвести до появи штучного інтелекту, який знаходиться поза контролем людини, що призводить до непередбачуваних і потенційно небезпечних результатів.

Використання штучного інтелекту також надає можливість для тотального спостереження та стеження за кожним громадянином, де окремі особи та суспільства піддаються постійному моніторингу та контролю.

Використання та розвиток ШІ не обмежується окремими країнами, що призводить до глобалізації ШІ та необхідності міжнародного співробітництва та регулювання його розвитку, впровадження та використання.

Різні підходи до розробки та впровадження ШІ, створення різноманітних реалізацій ШІ різними організаціями і країнами, можуть призвести до конфліктів і протистояння, як між країнами та організаціями у використанні, так і між різними реалізаціями ШІ. В результаті можуть виникнути як цілеспрямовані, так і спонтанні кооперація та протистояння між різними реалізаціями ШІ.

Це лише деякі виклики та загрози, пов'язані з ШІ. Важливо, щоб політики, дослідники, освітяни та інші зацікавлені сторони працювали разом, щоб вирішити ці проблеми та забезпечити відповідальне та етичне використання ШІ.

В цілому, повний перелік усіх викликів і загроз, пов'язаних зі штучним інтелектом (ШІ), надати не тільки важко, а й не можливо, оскільки сфера постійно розвивається і можуть виникати нові проблеми[26,27].

Протидія ризикам ШІ

Протидія ризикам, пов’язаним зі штучним інтелектом (ШІ), набуває надзвичайної важливості, оскільки розвиток ШІ потребує взаємодії та спільних дій всіх сторін, що займаються цими процесами. Це охоплює наукові, науково-дослідні, освітні, виробничо-промислові структури різних форм власності, державні і громадські установи, законодавчу і виконавчу владу, міжнародне співтовариство та інші організації. Метою такої співпраці є забезпечення безпечного високотехнологічного розвитку суспільства.

Необхідно створити ефективну систему виявлення загроз і оцінки ризиків, пов’язаних з розвитком і впровадженням штучного інтелекту та інших продуктів високих технологій у всіх сферах життєдіяльності суспільства. Це дозволить запобігти, стримати та нейтралізувати їх негативний вплив на людину, громадянина, суспільство, державу та міжнародне співтовариство.

Запропоновано комплекс заходів зниження ризиків та нейтралізації загроз, включаючи:

– Впровадження системи всебічного аналізу та оцінки загроз, пов’язаних з розвитком і використанням інноваційних високотехнологічних розробок загалом і штучного інтелекту зокрема.
– Аналіз та оцінка нормативно-правового забезпечення питань, пов’язаних з розвитком і використанням інноваційних високотехнологічних розробок загалом і штучного інтелекту зокрема, та визначення пріоритетних першочергових кроків щодо їх регулювання.

[26] Artificial Intelligence and National Security. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

[27] Artificial Intelligence Index Report 2023, Stanford Institute for Human-Centered Artifcial Intelligence, 2023, 385 p.

- Визначення шляхів сприяння організації та координації міжнародного і національного державно-приватного партнерства та співробітництва з питань забезпечення безпечності продуктів високих технологій та інновацій для людини, суспільства і держави.
- Організація дискусій щодо міжнародного та національного державно-приватного партнерства з питань безумовного забезпечення безпечності продуктів високих технологій та інновацій, зокрема штучного інтелекту, для людини, суспільства і держави.
- Здійснення інформаційно-аналітичного та експертного супроводження прогнозування розвитку та дослідження продуктів високих технологій і нових підходів до їх застосування з оцінкою ризиків та визначенням і реалізацією механізмів управління ними для безумовного забезпечення безпечності таких продуктів для людини і суспільства.
- Забезпечення підтримки безпечного створення, розвитку та впровадження штучного інтелекту в професійній, науковій, освітній та повсякденній діяльності для людини і суспільства.

Реалізація цих заходів, а також інших аналогічних заходів, дозволить сформувати систему попередження, зниження та нейтралізації загроз, пов'язаних з швидким розвитком високих технологій та інновацій, зокрема штучного інтелекту, для людини, суспільства і держави.

При цьому, для своєчасного і якісного вирішення цих питань важливо мати обґрунтовану базову систему індикаторів загроз штучному інтелекту як на глобальному і загальнодержавному рівнях, так і на відомчому та об'єктному рівнях. Особливу увагу слід приділяти об'єктам високого ризику, зокрема об'єктам критичної інфраструктури (ОКІ), а серед них — ОКІ сектору безпеки і оборони держави (СБО). Тому, при формуванні системи індикаторів загроз штучному інтелекту варто враховувати специфіку цих об'єктів критичної інфраструктури та об'єктів сектору безпеки і оборони.

Додатково слід відзначити, що формування системи індикаторів загроз штучному інтелекту повинно бути гнучким та динамічним процесом, який враховує швидкі зміни технологій та появу нових загроз. Крім того, важливо забезпечити ефективну координацію між різними державними органами, відомствами, компаніями та іншими зацікавленими сторонами для досягнення спільних цілей у сфері захисту від загроз, пов'язаних з штучним інтелектом.

При розробці комплексної державної політики щодо штучного інтелекту варто враховувати взаємозалежність пов’язаних з цим аспектів, складність технологічних умов, необхідних для просування в цій галузі, а також необхідність узгодження багатьох факторів та інтересів. Державна політика повинна ґрунтуватися на партнерстві на міжнародному та національному рівнях з метою створення екосистеми штучного інтелекту, яка сприяє сталому розвитку людей, суспільства і держави.

Особлива увага має бути приділена зниженню ризиків, пов'язаних з застосуванням штучного інтелекту у сфері кібербезпеки. З одного боку, штучний інтелект може бути ефективним інструментом для захисту від кіберзагроз, але з іншого боку, він сам може бути об'єктом деструктивних впливів з непередбачуваними наслідками. Особливо небезпечними є неконтрольовані дії штучного інтелекту в цій сфері, зокрема у відношенні об'єктів критичної інфраструктури, державних систем та військових мереж. Тому важливо розробити сучасні системи для виявлення, аналізу та нейтралізації таких дій, включаючи системи автоматичного виявлення нештатної або аномальної поведінки штучного інтелекту.

Для протидії використанню штучного інтелекту у злочинній, маніпулятивній або шпигунській діяльності необхідно розробити програмно-алгоритмічні комплекси для виявлення та відстеження недостовірної інформації, розпізнавання підроблених даних та забезпечення цілісності систем штучного інтелекту. Такі заходи гарантують надійний захист інформації, даних та систем, що використовують штучний інтелект у контексті національної безпеки і оборони.

Ефективна міжнародна співпраця та стандартизація мають велике значення в цьому контексті. Це дозволяє об'єднати зусилля, обмінюватися передовими практиками та розробляти спільні підходи до використання штучного інтелекту, забезпечуючи ефективність і синергію дій країн на глобальному рівні. Стандарти повинні встановлювати етичні принципи, правові рамки та норми поведінки для використання штучного інтелекту в контексті безпеки і оборони. Вони також сприятимуть забезпеченню взаєморозуміння між країнами, уніфікації підходів та забезпеченню безпеки і стабільності на міжнародному рівні.

У зв'язку з розглянутими викликами і загрозами, можна зробити висновок, що необхідний комплексний підхід до мінімізації ризиків і перетворення штучного інтелекту на надійний та безпечний інструмент для вирішення питань держави і суспільства.

Висновки

У статті детально розглянуто різні аспекти впливу штучного інтелекту на людину, громадян, суспільство і державу. Штучний інтелект має великий потенціал у вирішенні складних завдань у таких галузях, як національна безпека і оборона, медицина, наука, техніка та інших. Однак разом з цим, він може створювати серйозні загрози, такі як використання ШІ для нанесення шкоди людям або об’єктам, непідконтрольні дії ШІ, зміна балансу сил між державами та інші негативні наслідки.

Для запобігання загрозам, пов'язаним із штучним інтелектом, необхідно вжити комплекс заходів. Важливо забезпечити формування необхідного нормативно-правового забезпечення, а також системи попередження, зниження та нейтралізації загроз штучного інтелекту, особливо щодо об'єктів критичної інфраструктури та сектору безпеки і оборони. Також варто розвивати базову систему індикаторів загроз штучного інтелекту на різних рівнях.

У сфері національної безпеки і оборони штучний інтелект має як позитивний внесок, так і нові виклики, ризики та загрози. За допомогою розвитку кадрового потенціалу, покращення кіберзахисту та міжнародної співпраці і стандартизації можна ефективно використовувати штучний інтелект в інтересах національної безпеки і оборони. Навчання та підготовка фахівців з штучного інтелекту, розробка сучасних систем кібербезпеки та спільна робота з іншими країнами є основою для успішного застосування цієї технології. При цьому важливо враховувати етичні та правові аспекти використання штучного інтелекту, а також геополітичні наслідки.

Результативне реагування на виклики штучного інтелекту для національної безпеки і оборони вимагає постійного вдосконалення, інновацій та співпраці між державами. Лише поєднуючи зусилля, спільну роботу та встановлення міжнародних стандартів, ми зможемо забезпечити безпеку, стабільність та захист національних інтересів в епоху штучного інтелекту.

Загалом, штучний інтелект є важливим напрямком розвитку технологій, але для максимальної користі від його використання необхідно приділити увагу питанням безпеки та етики. Для ефективного використання штучного інтелекту в галузі національної безпеки і оборони необхідно розвивати етичні стандарти, забезпечувати безпеку та конфіденційність даних, вирішувати питання відповідальності за автономні системи, а також розуміти геополітичні наслідки розвитку штучного інтелекту. Технології штучного інтелекту можна вважати складовою системи забезпечення національної безпеки і оборони, враховуючи їх важливість для всіх сфер діяльності та темпи розвитку.