УДК 004.8:355(477)
https://doi.org/10.34142/23121661.2023.38.05
orcid. org/0000-0002-6019-1086

Т.А. Павленко

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНОЗДАТНОСТІ УКРАЇНИ: ПЕРСПЕКТИВИ СТРАТЕГІЇ РОЗВИТКУ

T. Pavlenko

USE OF ARTIFICIAL INTELLEGINCE TECHNOLOGIES IN PROVIDING NATIONAL SECURITY AND DEFENCE CAPABILITY OF UKRAINE: PROSPECTS OF DEVELOPMENT

Анотація. У статті розглянуто роль, місце та важливість використання технологій штучного інтелекту в гарантії національної безпеки України та її напрямів, а також обороноздатності нашої країни. Наголошено на важливості впровадження досвіду зарубіжних країн щодо швидкого, ефективного та гнучкого забезпечення потреб суспільства у воєнній безпеці та обороноздатності держави у період збройної агресії та в повоєнний період шляхом впровадження новітніх технологій, зокрема технологій штучного інтелекту. Окрему увагу приділено питанню правового режиму штучного інтелекту та вивченню стратегічного бачення використання можливостей штучного інтелекту в гарантії національної безпеки, її напрямів та обороноздатності України. Зазначено, що сьогодні в нашій державі прийнято шість довгострокових документів у безпековому напрямі, що безпосередньо або опосередковано стосуються питань національної безпеки, обороноздатності нашої держави й певним чином торкаються проблем використання технологій штучного інтелекту та сучасних інформаційних технологій. Визначено, що Україна обрала європейський шлях цифровізації розвитку суспільства та поширення технологій штучного інтелекту. Разом з тим, встановлено, що єдиного стратегічного уявлення щодо напряму стратегічного розвитку технологій штучного інтелекту в сфері гарантії національної безпеки та її напрямів немає, що може негативно впливати на подальший процес упровадження таких технологій у забезпеченні національної безпеки та обороноздатності нашої країни.

Ключові слова. Штучний інтелект, правовий режим штучного інтелекту, національна безпека та обороноздатність України, права людини, захист персональних даних, кіберфізична система.

Annotation. The article considers the role, place and importance of the use of artificial intelligence technologies in providing national security of Ukraine and its directions as well as

defence capability of Ukraine. It is highlighted that implementation experience of foreign countries on fast, effective and flexible introduction of needs of society for military security and defence capability of country throughout the period of armed aggression and in the postwar period through introduction of new technologies and particularly artificial intelligence technologies is important. The special attention is paid to issues of legal regime of artificial intelligence and studying in strategic vision of the use of artificial intelligence opportunities in providing national security, its directions and defence capability of Ukraine. It is noted that there are currently six adopted long-term documents on defence direction that directly affect issues of national security, defence capability of Ukraine and in some way affect issues of the use of artificial intelligence technologies and modern information technologies. It is defined that Ukraine has chosen European way to digitalize society and spread artificial intelligence technologies. At the same time, it is established that there is no one and only strategic view on strategic development of artificial intelligence technologies in the field of providing national security and its directions, that can negatively affect further process of introducing of such technologies in providing national security and defence capability of Ukraine. It is noted that today artificial intelligence technologies are considered as those are developing rapidly and have a significant potential in many fields, including national security, defence, information security and cybersecurity, intelligence and counterintelligence, aerial reconnaissance etc. Therefore it is important to consider the problem of strategic direction in implementation of such technologies and it is important to take on board the experience of advanced countries of the world. It should be done given the importance and an absolute prospect of using such an instrument as artificial intelligence in the field of national security and defence capability.

Key words. Artificial intelligence, legal regime of artificial intelligence, national security and defence capability of Ukraine, human rights, protection of personal data, cyber-physical system.

Постановка проблеми. Безпека була та є базовою потребою будь-якої людини [19]. Усталена безпека це «одне із наріжних питань, яке поставало перед Україною впродовж її багатовікової історії. Повномасштабна відкрита збройна агресія російської федерації (далі – рф) проти України оголила численні загрози, що постали не тільки перед нашою державою, а і перед всією світовою системою безпеки в цілому» [1]. «Відтак, сфера оборони та безпеки в сучасному світі є галуззю номер один і вона зазнає серйозних змін від впровадження технологій штучного інтелекту, що змінює баланс сил між державами» [2, с. 16]. Зауважимо, що одним із чинників, який може сприяти забезпеченню національної безпеки нашої держави та її обороноздатності може стати саме застосування технологій штучного інтелекту.

Аналіз останніх досліджень і публікацій. Питанням ролі й місця штучного інтелекту у сфері кримінально-правових відносин приділено увагу в роботах В.А. Мисливого, М.В. Карчевського та Н.А. Савінової. Зокрема, М.В. Качевським було запропоновано огляд однієї з перших спроб систематизувати статистичні дані щодо протидії злочинності у форматі відтворюваного дослідження за методологією Data Science [3]. Значний внесок у

дослідження питання впровадження штучного інтелекту у сферу захисту національної безпеки та обороноздатності зробили такі науковці, як В.Є. Хаустова, О.І. Решетняк, М.М. Хаустов, В.А. Зінченко [4], З. В. Гбур [5], Ніно Пацурія [6] та ін.. Проте, кожне запропоноване науковцями дослідження відкриває нові проблеми та можливості для подальших наукових розвідок.

Метою статті є визначення важливості технологій штучного інтелекту та необхідності єдиного стратегічного бачення використання можливостей таких технологій у забезпеченні національної безпеки України та її напрямів, а також обороноздатності нашої держави.

Виклад основного матеріалу. Під штучним інтелектом прийнято розуміти «комплекс технологічних рішень, що дозволяє імітувати когнітивні функції людини та отримувати при виконанні конкретних завдань результати, що дорівнюють результатам інтелектуальної діяльності людини» [5]. Штучний інтелект являється результатом людської діяльності, він здатний до логічного мислення, навчання, управління своїми діями, обґрунтування своїх рішень.

У сфері національної безпеки і, особливо її окремого виду, – інформаційної безпеки, застосування штучного інтелекту розпочалось на початку 2000-х років із достатньо простих речей. А саме, «побудови систем, що полегшують роботу спеціалістів певного профілю, зокрема вірусних аналітиків. До певного часу кількість зразків шкідливих файлів стала настільки великою, що ручним або простим автоматизованим аналізом уже було не обійтися. Це були системи, які виявляють паттерни в шкідливому коді та дозволяють проводити хоча б мінімальну атрибуцію» [7, с. 133].

Як правило, «використання штучного інтелекту в інформаційній безпеці обумовлено насамперед двома чинниками: необхідністю оперативного реагування під час настання кіберінциденту; нестачею кваліфікованих спеціалістів з кіберзахисту» [8, с. 10]. Разом із тим на сучасному етапі розвитку нашого суспільства ми можемо говорити про доволі широке використання штучного інтелекту у сфері інформаційної безпеки, зокрема, і національної безпеки загалом. Наприклад, «є глобальні компанії, які аналізують в мережі великий обсяг інформації, що може вказувати на нові загрози або, до прикладу, передбачити атаки нульового дня. Штучний інтелект також застосовується у відслідковуванні загроз, де за його допомогою на основі інформації, яка зібрана з відкритих та закритих джерел, прогнозуються загрози інформаційній безпеці» [5]. Так, «штучний інтелект може допомогти в проведенні аналізу дуже значної кількості розвідданих з відкритим вихідним кодом, що виходить з України (від відео TikTok і повідомлень в Telegram про формування військ і проведення атак, які завантажуються пересічними українцями, до загальнодоступних супутникових знімків), що дозволить групам громадянського

суспільства перевіряти претензії, що висуваються обома сторонами збройної агресії рф, а також документувати військові злочини та порушення прав людини. Крім того, фахівці вважають, що такі методи штучного інтелекту, як deepfakes можуть ставати дуже реалістичними відеофейками. Машинне навчання, як різновид штучного інтелекту, також може бути використане для виявлення дезінформації» [4, с. 18–19]. Тобто масштаб завдань та обсяг застосування штучного інтелекту у сфері інформаційної безпеки за останні роки збільшився в рази.

Зауважимо, що «досвід зарубіжних країн також доводить, що швидке, ефективне та гнучке забезпечення потреб суспільства у воєнній безпеці та обороноздатності держави у період збройної агресії та в повоєнний період досягається шляхом впровадження новітніх технологій, зокрема застосування штучного інтелекту та Big Data, як пріоритету подальшого розвитку оборонно-промислового комплексу України» [7, с. 134].

Крім того, результати досліджень Науково-технічної організації НАТО підтверджують важливість використання штучного інтелекту для забезпечення національної безпеки та обороноздатності, вони «визначають найбільш суттєві з них для розвитку технологій на найближчі 20 років. Зокрема, ключовими технологіями є: Big Data, штучний інтелект, автономні транспортні засоби, космос, гіперзвукові літальні апарати, квантові технології, біотехнології, нові матеріали та ін.» [4, с. 18].

Згідно з даними, що містяться в щорічних доповідях Стенфордського університету «Artificial Intelligence Index Report», «протягом останніх років багато держав розробили довгострокові національні Стратегії розвитку штучного інтелекту та здійснюють певні заходи щодо їхнього впровадження. Наприклад, Швейцарією в 2019 році підписано угоду з Thales Group3, якою передбачено поставку елементів центру обробки зображень IMINT4. Ця система дозволить збирати та аналізувати всі типи цифрових інформаційних зображень, а також включатиме провідні технології штучного інтелекту, що дасть змогу Збройним Силам Швейцарії ідентифікувати загрози та застосовувати адекватні моделі захисту» [9]. Навіть країна-агресорка (рф) зробила штучний інтелект своїм стратегічним пріоритетом в оборонних можливостях.

Що стосується України в контексті стратегічного бачення використання можливостей штучного інтелекту в гарантії національної безпеки та її напрямів, то маємо таку ситуацію. Сьогодні прийнято шість довгострокових документів у безпековому напрямі, що безпосередньо або опосередковано стосуються питань національної безпеки, обороноздатності нашої держави й певним чином торкаються проблем використання штучного інтелекту, Big Data та сучасних інформаційних технологій. Це Стратегія національної безпеки

України**,** згідно з положеннями якої «поточними та прогнозованими загрозами національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов є стрімкі технологічні зміни, насамперед в енергетиці та біотехнологіях, розробки у сфері штучного інтелекту, які докорінно трансформують економіку й суспільство загалом; розроблення системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері штучного інтелекту, створення нових матеріалів, робототехніки та автономних безпілотних апаратів» [10]. *Стратегія інформаційної безпеки [11], що визначає* «основними напрямами забезпечення інформаційної безпеки України протидію дезінформації та інформаційним операціям, насамперед держави-агресора. Стратегія кібербезпеки» [12] передбачає, що «забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, визначено, що реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі». Також затверджено *Стратегію забезпечення державної безпеки [13],* Стратегію воєнної безпеки України [14]**,** *Стратегію розвитку оборонно-промислового комплексу України [15].*

Також розпорядженням Кабінету Міністрів України №1556-р від 2 грудня 2020 року в Україні було схвалено Концепцію розвитку штучного інтелекту в Україні [16], яка «передбачає визначення основних напрямів та пріоритетних завдань розвитку технологій штучного інтелекту з метою забезпечення конкурентоспроможності національної економіки та захисту технологічних інформаційно-комунікаційних систем. Розпорядженням Кабінету Міністрів України від 12 травня 2021 року № 438-р затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки» [17], згідно до положень якого «на зазначений період передбачено низку заходів та законодавчих ініціатив, зокрема, запровадження правового регулювання з питань формування державної політики в галузі штучного інтелекту; упровадження технологій штучного інтелекту в національну систему кібербезпеки для проведення аналізу й класифікації загроз та вибору стратегії їхнє стримування й запобігання їх виникненню; визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту в документах оборонного планування та ін.» [17].

23 лютого 2023 року Верховна Рада України ратифікувала Угоду між Україною та ЄС про участь України в програмі ЄС «Цифрова Європа», «тим самим Україна підтримала європейський шлях цифровізації розвитку суспільства та поширення штучного інтелекту» [18].

Висновки. Сьогодні технології штучного інтелекту належать до таких, що стрімко розвиваються та мають значний потенціал у багатьох галузях, зокрема: національну безпеку, оборону, інформаційну та кібербезпеку, розвідку й контррозвідку, аеророзвідку тощо. І загалом в Україні на нормативно-правовому рівні сформовано бачення щодо застосування технологій штучного інтелекту у сфері національної безпеки та її напрямів. Разом із цим, єдиного стратегічного документу, який би запроваджував єдиний напрям стратегічного розвитку технологій штучного інтелекту у сфері забезпечення національної безпеки, наразі немає. На жаль, навіть не ведуться обговорення щодо не обхідності та перспективності розробки такого документу. Хоча, враховуючи важливість та безумовну перспективність застосування такого інструменту як штучний інтелект у сфері національної безпеки та обороноздатності, слід було б замислитися над цим питанням та взяти на озброєння досвід передових країн світу.

Література

1. Пацурія Ніно Впровадження технологій штучного інтелекту у забезпечення національної безпеки та обороноздатності України: проблеми та перспективи повоєнного періоду. 31.03.2023. URL: https://coordynata.com.ua/vprovadzenna-tehnologij-stucnogo-intelektu-u-zabezpecenna-nacionalnoi-bezpeki-ta-oboronozdatnosti-ukraini-problemi-ta-perspektivi-povoennogo-periodu. **2.** Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 4. С. 16–26. **3.** Карчевський, М. В.. Протидія злочинності в Україні у форматі DATA SCIENCE. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2022. 2(98) / С. 202-227. https://doi.org/10.33766/2524-0323.98.202-227. **4.** Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. *БІЗНЕСІНФОРМ*. 2022. № 3. С. 17−26. **5.** Гбур З. В. Використання штучного інтелекту в інформаційній безпеці України. *Державне управління: удосконалення та розвиток*. 2022. № 1. URL: http://www.dy.nayka.com.ua/?op=1&z=2601. **6.** Ніно Пацурія Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду. *Теорія і практика інтелектуальної власності*. 3/2023. С. 68-78. **7.** Павленко Т.А. Технології штучного інтелекту у забезпеченні інформаційної безпеки України. *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання : матеріали VII Міжнар. наук.-практ. конф., м. Харків, 11 трав. 2023 р. / [редкол.: Л. М. Демидова (голов. ред.), Н. В. Шульженко та ін.]*. – Харків: Право, 2023. С. 132–137. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/ ttps://ivpz.kh.ua/wp-content/uploads.pdf **8.** Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA. Int. J. Cyber Warf. Terror. 2016. Vol. 6. pp. 1–16. **9.** Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. URL: https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure. **10**. Указ Президент України від 14 вересня 2020 року № 392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію

національної безпеки України» URL: https://www.president.gov.ua/documents/3922020-35037. **11**. Указ Президент України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України» URL: https://www.president.gov.ua/documents/6852021-41069. **12**. Указ Президент України від 26 серпня 2021 року № 447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки безпеки України» URL: https://www.president.gov.ua/documents/4472021-40013. **13**. Указ Президент України від 16 лютого 2022 року № 56/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки України» URL: https://www.president.gov.ua/documents/ 562022-41377. **14**. Указ Президент України від 25 березня 2021 року № 121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» URL: https://www.president.gov.ua/documents/1212021-37661. **15**. Указ Президент України від 20 серпня 2021 року № 372/2021 Про рішення Ради національної безпеки і оборони України від 18 червня 2021 року «Про Стратегію *розвитку оборонно-промислового комплексу* України» URL: https://zakon.rada.gov.ua/laws/show/ 372/2021#Text. **16**. Концепція розвитку штучного інтелекту в Україні. Розпорядження Кабінету міністрів України № 1556-р від 02 грудня 2020. URL: https://zakon.rada.gov.ua/ laws/show/1556-2020-%D1%80#Text. **17**. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки. Розпорядження Кабінету міністрів України № 438-р від 12 травня 2021 р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text. **18**. Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027). URL: https://zakon.rada.gov.ua/ laws/show/984_005-22#n2. **19**. Pavlenko, M Korabel - The national security field under conditions of armed aggression of the Russian Federation against Ukraine in 2022 Journal of Geography, Politics and Society, 2022 p. 51-54.