МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин та суспільних комунікацій

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ЗАХИСТУ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Кваліфікаційна робота

Рівень вищої освіти – другий (магістерський)

Виконав:
студент 6 курсу, 604 групи
Горченко Валентин Вікторович
Керівник:
кандидат політичних наук,
доцент **Осадца І.С.**

До захисту допущено
на засіданні кафедри
протокол №____від _____ 2023 р.
Зав. кафедрою _____ доц. Макар В.Ю.

Чернівці – 2023

Анотація

Магістерська робота присвячена дослідженню питань захисту кібернетичної безпеки держави з огляду на стрімкий розвиток та поширення можливостей штучного інтелекту.

У XXI столітті, в епоху в першу глобалізації, проблема функціонування різних інформаційних систем стала в один ряд із проблемами перенаселення та глобального потепління. Насамперед це пов’язано із надактивним розвитком штучного інтелекту.

Також слід зазначити на важливості використання штучного інтелекту в Україні наразі саме в умовах захисту та наступу на російські окупаційні війська, проте в умовах воєнного стану проблема формування цілісної концепції адміністративно-правового механізму реалізації правової доктрини у сфері штучного інтелекту знайде свою реалізацію у період післявоєнної відбудови України.

У роботі розглянуто теоретико-методологічні основи дослідження використання можливостей штучного інтелекту в кібернетичній безпеці держави, адміністративні, нормативно-правові засади впровадження штучного інтелекту у різні сфери людської діяльності. Особливу увагу було зроблено на аналізі впровадження та використання штучного інтелекту в Україні, насамперед з огляду на військові дії.

Ключові слова: штучний інтелект, кібернетична безпека держави, сфери використання штучного інтелекту, обороноздатність країни.

Summary

The master's thesis is devoted to the study of issues of protection of the cybernetic state in view of the rapid development and opportunities for the development of the security of artificial intelligence.

In the 21st century, in the era of the first globalization, the problem of the functioning of various information systems became one with the problems of overpopulation and global warming. This is primarily due to the overactive development of artificial intelligence.

We also note the importance of the use of artificial intelligence in Ukraine at the moment precisely in the conditions of protection and attack on the Russian occupying forces, however, in the conditions of martial law, the problem of forming a holistic concept of the administrative-legal mechanism for the implementation of the legal doctrine in the field of artificial intelligence will find its implementation in the period of post-war reconstruction of Ukraine. .

The work considers the theoretical and methodological foundations of the study of the possibilities of using artificial intelligence in the cyber security of the state, administrative, normative and legal measures for the introduction of artificial intelligence in various spheres of human activity. Special attention was paid to the analysis of the introduction and use of artificial intelligence in Ukraine, primarily with regard to military operations.

Keywords: artificial intelligence, cyber security of the state, field of use of artificial intelligence, defense capability of the country.

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело.

_____ Прізвище І.П.
(підпис)

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Конституція України у ч. 11 ст. 92 проголосила, що виключно законами України визначається організація і діяльність органів виконавчої влади, основи державної служби, організації державної статистики та інформатики. Таке положення Основного Закону ще у 1996 році фактично закріпило основи того, що інформатизація є настільки важливою, що вона має визначатися виключно законами України.

У XXI столітті, в епоху в першу глобалізації, проблема функціонування різних інформаційних систем стала в один ряд із проблемами перенаселення та глобального потепління. Насамперед це пов'язано із надактивним розвитком штучного інтелекту.

Згідно з вибірковим опитуванням 7502 підприємств у всьому світі, проведеним 30 березня – 12 квітня 2022 року компанією Morning Consult на замовлення IBM, світова частка підприємств, що впровадили штучний інтелект, наразі становить 35%, збільшившись на 4 процентні пункти з 2021 року. У Китаї та Індії найвищі показники розгортання штучного інтелекту – 58 % і 57 % відповідно, тоді як у Канаді – 28 %, у Великобританії – 26 %, у США – 25 % і в Південній Кореї – 22 %. З опитаних підприємств 28% мають цілісну стратегію штучного інтелекту, 25 % зосереджені лише на обмежених або конкретних випадках використання, а 37 % розробляють стратегію штучного інтелекту.

Актуальність даного дослідження перш за все обумовлена стрімкими темпами росту впровадження у всі сфери життя штучного інтелекту. Це обумовило як захоплення можливостями штучного інтелекту так і побоювання в суспільстві щодо можливих наслідків його використання. Тому постає проблема захисту безпеки держави від наслідків використання ШІ. Особливо це яскраво стало проявлятися останніми роками в контексті розвитку інформаційних технологій та використання ними систем штучного інтелекту. Провідні IT-гіганти наввипередки змагаються в тому чия система

ШІ краща, забуваючи іноді про те, що вона може нести небезпеки суспільству, країні, людині.

Показовим в цій ситуації стало рішення найбільших концернів світу та провідних політиків розвинених країн щодо регулювання та обмеження використання можливостей штучного інтелекту.

Також слід зазначити на важливості використання штучного інтелекту в Україні наразі саме в умовах захисту та наступу на російські окупаційні війська, проте в умовах воєнного стану проблема формування цілісної концепції адміністративно-правового механізму реалізації правової доктрини у сфері штучного інтелекту знайде свою реалізацію у період післявоєнної відбудови України.

Мета і завдання дослідження. Метою дослідження є визначення ролі та значення, переваг і недоліків штучного інтелекту у питаннях посилення стану кібербезпеки держави.

Для досягнення поставленої мети потрібно вирішити такі **завдання**:

– розглянути сучасний стан та наукові розробки дослідження ролі штучного інтелекту в кібернетичній безпеці держави;

– розкрити адміністративні та нормативно-правові засади впровадження технологій штучного інтелекту в кібернетичній безпеці держави;

– охарактеризувати особливості використання штучного інтелекту у питаннях забезпечення кібернетичної безпеки держави;

– описати сфери можливого використання штучного інтелекту у кібернетичній безпеці держави;

– проаналізувати останні тенденції розвитку штучного інтелекту в Україні.

Об’єктом дослідження є методи та інструменти втілення штучного інтелекту в безпековій політиці.

Предметом дослідження є роль штучного інтелекту як інструменту захисту кібернетичної безпеки держави.

Методи дослідження обрано на основі визначених у роботі мети й завдань, з урахуванням її об’єкта і предмета. Серед основних підходів варто виокремити такі: системний підхід, який використовувався для розгляду системи впровадження, регулювання та використання штучного інтелекту в кібернетичну безпеку держави. Він дозволяє враховувати взаємозв’язки та вплив різних чинників на динаміку впровадження новітніх технологій штучного інтелекту в різні сфери людського життя. Історичний підхід був застосований для аналізу зародження і розвитку штучного інтелекту. Інституціональний підхід використовувався для ретельного розгляду та аналізу інформації з метою визначення тенденцій, особливостей впровадження штучного інтелекту в кібернетичну безпеку держави.

За допомогою діалектичного методу визначено сутність і зміст механізму впровадження та реалізації системи штучного інтелекту в кібернетичний захист держави. За допомогою законів формальної логіки визначено елементи адміністративного механізму реалізації правової доктрини у сфері штучного інтелекту в Україні, нормативно-правового регулювання технологій штучного інтелекту. Компаративний метод дозволив систематизувати практику використання та регулювання штучного інтелекту в закордонних країнах. Метод узагальнення використовувався для формулювання висновків та визначення загальних тенденцій на підставі отриманих результатів. Наше дослідження включало в себе і використання окремих наукових методів, спрямованих на докладний аналіз та розуміння останніх тенденцій використання штучного інтелекту в кібернетичній безпеці держави, особливо з огляду на цифровізацію системи державного управління країни та війни України з Російською Федерацією.

Структура та обсяг роботи. Дослідження складається з анотації, вступу, трьох розділів, які об’єднують 7 підрозділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 114 сторінок, з яких основний текст роботи займає 92 сторінки, список використаних джерел та літератури розташований на 14 сторінках (109 найменувань).

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Сучасні наукові підходи дослідження ролі штучного інтелекту в кібернетичній безпеці держави.

Активне впровадження та використання штучного інтелекту за останні роки в різних сферах діяльності людини, неоднозначність інтерпретації поняття штучного інтелекту призводить до викривленого та неоднозначного трактування штучного інтелекту. Сьогодні навряд чи можна здивувати визначенням «штучний інтелект» навіть пересічного громадянина. Однак, вчені вже десятиріччями ведуть запеклі суперечки з приводу існування штучного інтелекту. За цей час створені програми для встановлення виміру штучного інтелекту, тобто здатності «машини» на роздуми, відчуття, емоції, пізнання, розуміння і це все одночасно, тобто такі процеси, які відбуваються у діяльності людини. Спільні зусилля вчених різних галузей протягом кількох десятиліть спрямовані на вирішення складної задачі – розуміння поняття «штучний інтелект».

Починаючи пошуки розуміння штучного інтелекту, необхідно звернутись до філософського виміру «інтелект людини» та «свідомість особистості», за для виділення генези розглядуваного поняття, оскільки вчені до теперішнього часу ведуть дослідження з метою з’ясування поняття інтелект людини та свідомість особистості. Ці питання виникали у людей ще за часів зародження філософії, і до теперішнього часу вчені намагаються встановити розуміння цих понять, дати остаточне визначення.

Перші визначення поняття «штучний інтелект» дає ще у 1956 році американський фахівець з інформатики та дослідник мислення Джон Маккарті. Однак, варто зазначити, що до остаточного впровадження терміну «штучний інтелект» проводились впровадження щодо інтелекту перших електронно-обчислювальних машин. Значний внесок був зроблений англійським математиком Аланом Тьюрінгом, який першим запровадив тест

щодо здатності ЕОМ мислити, як людина. Цей тест увійшов в історію розвитку «штучного інтелекту» під назвою автора тест Тьюрінга.

Кінець XX – початок XXI століття ознаменувалися активним періодом розвитку технологічного процесу, особливо стрімко іде розвиток за останні роки завдяки IT технологіям. Сьогодні складно уявити своє життя без технологічних засобів, оглядаючись на минуле, покоління людей дивуються, як можна було обходитись без звичних на сьогодні речей. Заповнюючи наше середовище в повному обсязі важно знайти людей, які не користуються IT технологіями, це скоріш виходить за рамки нормальної поведінки, чого не можна сказати ще 10 років назад.

В Штатах Америки запровадження IT технологій відбулось значно раніше ніж в Україні. Вже після активного впровадження технологічного процесу виникає питання щодо визначення штучного інтелекту, як у філософському так і правовому напрямках. За останні роки в Україні також активно впроваджується технологічний процес. Звичайно розвиток технологій відбивається на звичний порядок життя, такі як професійна, побутова, дозвільна, виховна сфери та інші [4].

Штучний інтелект сягає своїм корінням в давнину. Перші дослідження, пов’язані з процесами мислення, здійснювались у філософії. Принципи раціонального мислення були сформульовані ще Аристотелем (384 – 322 до н. е.). У XVI столітті Рене Декарт вперше поділився своїми висновками про відмінності між розумом і матерією. Філософія спрямувала увагу на ключові принципи, що керують раціональною частиною мислення, а математика на формалізацію цих принципів та глибокі наукові дослідження. Протягом багатьох століть обидві ці галузі науки розвивалися паралельно, взаємно вдосконалюючи одна одну. На штучний інтелект найбільший вплив мав розвиток таких розділів математики як логіка, обчислення та ймовірність [12, с. 185].

Не можна зрозуміти поняття «штучний інтелект», не розглянувши інтелект людини. Так, інтелект (від лат. intellectus – розуміння, розум,

пізнання) – «відносно стійка структура розумових здібностей індивіда. Зазвичай інтелект визначають за рівнем розвитку, який розглядають у зв'язку з такими пізнавальними процесами, як сприймання, пам'ять, уява тощо». Трактування інтелекту як загальних розумових здібностей використовують у вигляді поведінкових характеристик індивіда, пов'язаних з розумінням та прогнозуванням подій, ефективністю діяльності, успішною адаптацією до нових життєвих завдань [9].

В середньовіччі філософи ідеалісти та матеріалісти пов'язували поняття інтелекту людини з його природними, вродженими розумовими здібностями. З часом інтелект розглядався з урахуванням основ психології. В XX сторіччі інтелект розглядається з медичної точки зору та в розрізі досліджень мозкової діяльності людини. Такі комплексні дослідження дали змогу вченим наблизитись до розв'язання давньої проблеми з'ясування інтелекту. В решті це може вплинути на витоки поняття «штучний інтелект» та з'ясування його природи походження та тісного зв'язку із інтелектом людини.

Вже протягом тривалого часу вчені вступають у дискусії щодо самої природи цього поняття, оскільки вже існують програми для оцінювання штучного інтелекту, як здатності «машин» відтворювати роздуми, відчуття, емоції, навчання та розуміння, і все це одночасно, в усіх аспектах людського життя. Так, на думку Григоренко І.В.: «інтелект можна визначити як здатність особистості, яка зумовлює загальну успішність пристосовування людини до нових умов існування. Інтелект стає однією з найбільш суттєвих і необхідних властивостей особистості у сучасному суспільстві знань, яке активно формується у світі, що глобалізується. Перспективи подальших вбачаємо у детальному аналізі філософського аспекту інтелектуальної поведінки людини у сучасному соціумі» [8, с. 120].

Всі проведені дослідження природи штучного інтелекту торкаються у співставленні з інтелектом людини. Так, для створення штучного інтелекту необхідно виявити властивості природного інтелекту та розробити спосіб

його моделювання. У літературі подано багато означень штучного інтелекту, але точного визначення ще немає. Під інтелектом розуміють здатність пізнавати навколишній світ та вирішувати різноманітні проблеми. Як синонімом користуємося поняттям «розум», яке виражає здатність мислити, тобто аналізувати й робити висновки. Одним з понять штучного інтелекту вважають формалізацію проблем та завдань, які подібні до дій, що виконує людина. Різні автори природний інтелект моделюють по-різному. Наприклад, штучний інтелект визначається як властивість цифрової обчислювальної машини реагувати на інформацію, яка поступає на її вхідні пристрої, майже так, як реагує в тих же інформаційних умовах певна людина. Такий підхід ґрунтується на принципі самоорганізації моделі і його називають евристичний. У роботі інтелект людини розглядається як інтуїтивна система. Тобто, під інтуїцією розуміють процес оптимального прийняття рішень по відношенню до зовнішнього середовища [52].

Пройшовши шлях дослідження штучного інтелекту від появи самої ідеї до втілення та активного застосування за останні десятиріччя лише у 2020 році було схвалено Концепцію розвитку штучного інтелекту в Україні, яка закріпила поняття штучного інтелекту, як «організовану сукупність інформаційних технологій, із застосуванням якого можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [22].

Розглянувши різні точки зору можемо зазначити, що питання розвитку та становлення штучного інтелекту вченими розглядалось під різними кутами. Звісно, у контексті використання штучного інтелекту для розв’язання виробничих завдань в сільському господарстві, сфері послуг, освітній сфері, ІТ та інших галузях виникають питання, чи обмежується це лише виконанням програмованих завдань для полегшення їх реалізації, або чи

можливий перехід до рівня, коли штучний інтелект наближається до рівня інтелекту людини в плані здатності приймати незалежні рішення, усвідомлення загроз та небезпек.

Якщо говорити про якісні характеристики штучного інтелекту, то варто зазначити, що штучний інтелект давно вийшов за рамки розумових здібностей людини. Можна навести приклад, примітивного калькулятора із минулого сторіччя, однак навряд чи пересічний громадянин за декілька секунд зможе дати правильне рішення, наприклад множення з тризначними цифрами. Однак, людина здатна до прийняття нестандартних (незапланованих) рішень, може діяти на інтуїтивному рівні, інколи за відсутності логічності та послідовності і таке прийняте рішення буде в конкретній ситуації правильним. Да, за останні роки машини, наділені такими програмами, які можуть самостійно обрати шлях для досягнення поставленої мети, однак все одно не можуть вийти за рамки програми. Така програма передбачає декілька ситуацій при яких машині необхідно обрати шлях і прийняти відповідно до об'єктивної ситуації єдине вірне рішення. Ну самим головним необхідно пам'ятати, що всі технології штучного інтелекту створюється завдяки розумовим здібностям людини і звичайно націлені на службу саме людству.

Визначення, використані в данный роботі, враховують положення Концепції розвитку штучного інтелекту в Україні [19]. Разом з тим, Стратегія є наступним кроком реалізації сформульованих у Концепції завдань і передбачає більш глибоке осмислення змісту поняття «штучний інтелект», що базується на застосуванні принципів і механізмів функціонування мозку людини, зокрема її свідомості та совісті.

Термін «штучна свідомість» був уведений у науковий обіг іще в 1992 році [73]. Надалі проблему штучної свідомості досліджували зарубіжні фахівці Джон Кільстрем, Аніль Сет, Станіслас Деан, Майкл Граціано, Тейлор Вебб та інші [90]. Українські науковці розпочали такі дослідження в 2002 році, коли Анатолій Шевченко зробив доповідь на Міжнародній конференції

«Штучний інтелект» про підходи до проблеми моделювання штучного інтелекту та штучної свідомості [68].

Українська наукова школа штучного інтелекту розглядає свідомість людини як фундаментальну соціально-когнітивну систему, що є продуктом діяльності її мозку і спроможна сприймати й розпізнавати інформацію, формувати й систематизувати знання, самонавчатися, приймати самостійні мотивовані рішення залежно від поставлених завдань і наявних обставин, ураховуючи закони та правила соціуму. Свідомість формує особистість людини.

Поняття штучної свідомості передбачає наявність штучної совісті як механізму забезпечення етичності рішень ШІ. Це питання було позитивно сприйнято на засіданні Групи урядових експертів з питань летальних автономних систем озброєнь Управління ООН з питань роззброєння 27 червня 2022 року.

Як прототип штучного інтелекту взято інтелект людини. При цьому було проведено аналіз понад 50 наявних на сьогодні означень штучного інтелекту. Розглянемо деякі з них, що адекватно відображають сучасне бачення цього поняття.

Енциклопедія «Брітанніка» трактує штучний інтелект як «здатність цифрового комп'ютера або робота, контрольованого комп'ютером, вирішувати завдання, зазвичай пов'язані з розумними істотами» [76].

Міжнародний стандарт ISO/IEC TR 24028:2020 розглядає штучний інтелект як «здатність інженерної системи набувати, опрацьовувати та застосовувати знання та вміння» [79].

Словник Коллінза розглядає штучний інтелект як «тип комп'ютерної технології, яка спрямована на те, щоб машини працювали розумним чином, подібно до того, як працює людський розум» [77].

Оксфордський словник означує штучний інтелект як «здатність комп'ютерів або інших машин демонструвати або імітувати розумну поведінку; область дослідження, що стосується цього» [78].

Самого визначення «штучний інтелект» на сьогодні вже недостатньо, наукові дослідження пішли значно дальше ніж просте закріплення такого поняття. Питання співставлення поняття «штучний інтелект» та «інтелект людини» чи можна їх ототожнювати? Питання безпеки використання штучного інтелекту та наділення машин цією технологією стоїть дуже гостро і не лише в уяві, але і реально.

Питання, чи зможе штучний інтелект перевершити людей у майбутньому та які наслідки це може мати для суспільства, залишається досить дискусійним. Багато експертів зі штучного інтелекту висловлюють серйозні занепокоєння стосовно можливого негативного впливу цієї технології на суспільство та закликають дослідників глибше дослідити соціальний вплив штучного інтелекту. Могутня і всеосяжна роль сучасних технологій штучного інтелекту знову і знову викликають сумніви [27].

Так, О. Стеблинська загострює увагу на протиріччях та нестиковках, що пронизують сферу штучного інтелекту на глибинному рівні. По-перше, існує нечіткість у визначенні самого поняття «штучний інтелект». У книзі «Штучний інтелект: сучасний підхід» від С. Рассела і П. Норвіга відзначається, що різні визначення можна класифікувати за двома основними категоріями: одні описують мисленнєві процеси та методи розумової діяльності, інші – активності та поведінку. В одних визначеннях успіх вимірюється точним відтворенням людських здібностей, тоді як інші підкреслюють досягнення у контексті раціональності та логіки. Неоднозначним є застосування і самого терміна «інтелект». Якщо під цим терміном ми розуміємо лише розрахункові можливості людини, то штучний інтелект ефективно виконує обчислювальні завдання. Але якщо ми розглядаємо «інтелект» в більш широкому контексті, включаючи людські емоції, почуття, інтуїцію, творчість, уяву, етичні цінності та як духовний аспект, то досягнення такого «інтелекту» стає надзвичайно складним завданням і вимагає досягнення рівня свідомості, подібного до людської. [47].

Такі сучасні мислителі, як Дж. Серл, Д. Деннет, Д. Чалмерс, Р. Доукінз, П. та П. Черчленди, загострюють body-mind problem та висловлюють власні погляди на можливості реалізації свідомості на штучному носії. Це породжує питання: як можемо ми намагатися втілити в життя щось, чого не розуміємо повністю та не маємо чіткого уявлення про його сутність?! [47].

У сфері штучного інтелекту, практичне застосування має вагоміший вплив, ніж лише теоретичні можливості. У дослідженнях сфери штучного інтелекту особливе місце посідає філософська проблематика. Точніше, філософсько-епістемологічні дослідження цієї проблематики, які дозволили поглибитися у сутність процесів мислення та пізнання, переглянути підходи до інтелектуальної, зокрема творчої, діяльності та сприяли визначенню можливості їх комп'ютеризації [51].

Незважаючи на явний прогрес у розвитку та використанні штучного інтелекту, людей не полишають сумніви щодо такого активного використання штучного інтелекту та наділення його свідомістю задля прийняття конкретних рішень. Такі сумніви стосуються передбачуваної можливості машини вийти за межі програми та зашкодити суспільству.

Так, майбутні можливості цієї передової технології можна прирівняти до відомого міфу про скриньку Пандори. Однак, ми знаємо вміст скриньки Пандори, в той час як майбутнє штучного інтелекту залишається досить неочевидним [27].

Як ми бачимо чимало питань виникає щодо сутності існування штучного інтелекту та побоювання людства з приводу інтелектуальних переваг машин, які присутні у всіх сферах життя людини: побутовій, повсякденній, професійній, пізнавальній, навчальній та ін. Сумніви людей відображаються при створенні кінофільмів з демонстрацією ситуацій щодо переваги роботів над людьми, відеоігри тощо [44].

У заключному звіті з дослідження взаємосумісності спільної стратегії повітряних сил BI-SC Final Report on the Joint Air Power Strategy Interoperability Study (JAPS-IS) від 15 січня 2020 року використано означення,

запропоноване NIAG SG-231: «Штучний інтелект – здатність небіологічної системи досягти будь-якої складної мети за допомогою процесів, порівняних із когнітивними процесами людини, таких як сприйняття, дедукція, розпізнавання, запам'ятовування та навчання». Перше з офіційних означень НАТО (NATO adopted) було включене в настанову AJP3.10 Ed. B, Ver. 1. Allied Joint Doctrine for Information Operations. У її проєкті, датованому травнем 2021 року, в переліку термінів зазначено, що штучний інтелект – це «розділ інформатики, присвячений розробці систем аналізу даних, які виконують функції, зазвичай пов'язані з людським інтелектом, такі як міркування, навчання та самовдосконалення» [69].

Сучасні комп'ютери та суперкомп'ютери володіють потужністю, яка дозволяє ефективно виконувати надскладні математичні операції та вже давно перевищує людський інтелект у сенсі обчислювальних можливостей. Проте, незважаючи на цю високу обчислювальну потужність, важливо розуміти, що комп'ютери не мають інтелекту у справжньому розумінні. Обчислювальна потужність є лише однією з складових інтелекту, а її збільшення само по собі не призводить до виникнення інтелекту [69].

Вже декілька десятиліть перед науковцями стоїть складна задача визначення поняття «штучний інтелект» та співставлення з інтелектом людини, а також витоки походження штучного інтелекту та актуальність застосування штучного інтелекту в умовах сьогодення.

«Штучний інтелект – це програмний продукт, який отримує певний запит, збирає та обробляє дані, а потім видає готове рішення. Таке рішення часто сприймається, як результат роботи програми, яка демонструє інтелектуальну поведінку та працює подібно до людського мислення» [98]. Таке визначення із технічної точки розу дає відображення штучного інтелекту, як готового програмного продукту для використання машини в разі швидкого та чіткого прийняття рішення.

Завдяки кожному новому кроку у розвитку штучного інтелекту, наше усвідомлення власної природи стає глибшим. Чим більше ми намагаємось

створити штучний інтелект, тим більше ми осмислюємо складність та унікальність нашої свідомості та інтелектуальної природи.

Так, О. Е. Радутний в своїй роботі [42] робить переваги використання штучного інтелекту і зазначає, що «завдяки роботизації та автоматизації рутинних або ризикованих процесів людина поступово усувається від процесу обробки інформації, прийняття рішень та їх реалізації. У багатьох випадках це є цілком виправданим, адже все більше стає неможливим конкурувати з алгоритмами штучного інтелекту, які саме призначені для того, щоб перевершити людину у конкретно визначеній діяльності, усунути людський фактор у вигляді похибок, помилок та недосконалостей когнітивних функцій (слабка пам’ять, концентрація уваги, піддатливість до стресу тощо) та фізичних можливостей (сила, витривалість, сприйняття всіх сигналів оточуючого світу тощо)» [43].

Продовжуючи тему застосування штучного інтелекту не можна не торкнутись певних проблем, які можуть виникати. Так, О. Стебельська зазначає, що «серед основних проблем, з якими стикаються науковці, намагаючись створити розумні машини, можна відзначити такі: створюючи інтелектуальні машини, науковці не можуть наділити їх розумінням, у тому числі розумінням самих себе (або самосвідомістю); другою перепоною на шляху створення штучного інтелекту є проблема невизначеності: – ми живемо у плинному світі, який постійно змінюється; невід’ємною складовою частиною людини є її тілесність, через призму якої вона здатна сприймати світ, в якому живе; складною проблемою в процесі реалізації штучного інтелекту є ціннісний вимір людини; проблема відповідальності чітко взаємопов’язана з проблемою свободи; ще однією причиною тих труднощів, з якими стикаються дослідники, є природа квалій («незвичайний термін для позначення звичної для нас речі: того, як речі виглядають для нас»); однією з провідних особливостей людини є творчий характер її діяльності, здатність створювати щось таке, чого до неї в природі не існувало та існувати не могло; люди часто діють і роблять висновки, спираючись на здоровий глузд»

[47].

Розглянувши питання визначення поняття «штучний інтелект» в різних аспектах, можемо зазначити, що шлях у десятиріччя доволі складний і суперечливий. Так, звичайно є побоювання щодо проведення аналогії з людським інтелектом у буквальному розумінні, що може призвести до хибного визначення. Потрібно враховувати той факт, що до сьогодні неможливо точно визначити та виміряти людський інтелект.

Отже, якщо дослідження штучного інтелекту проводяться останні десятиліття, то осягнути розуміння та можливості людського інтелекту не вдається ще з античних часів, тисячоліття. Проводячи паралель, можемо зазначити, що так само складно і суперечливо буде проходити пізнання штучного інтелекту та його нормативне закріплення.

1.2. Аналіз джерельної бази дослідження.

Доцільно вказати, що деякі теоретичні та практичні питання використання ШІ у кібернетичній сфері в Україні та зарубіжних державах раніше вже розглядалися у науковій літературі. Так, наприклад, технічну компоненту та особливості використання систем ШІ в контексті забезпечення кібербезпеки розглядали у своїх наукових працях: О. Неретін та В. Харченко [26], В. Савченко та О. Шаповаленко [66], І. Стьопочкіна та О. Новіков [50]. Перспективні можливості ШІ як важливого механізму автоматизованої та негайної реакції на розвиток та модифікацію кіберзагроз вивчав С. Шаров [67]. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій ШІ у кібербезпеці здійснював С. Цяпа [62]. У зарубіжній науковій літературі роль та значення ШІ у сфері кібербезпеки та подальші шляхи його розвитку досліджували: Т. Сіпола [108], Р. Мостіну [93], Р. Дас та Р. Сандхейн [96].

Проте питання використання ШІ у сфері кібербезпеки недостатньо досліджено на науковому рівні. Особливо це відчувається в умовах появи у листопаді 2022 року феномену генеративного ШІ – ChatGPT та триваючого

(протягом останніх 22 місяців) правового режиму воєнного стану, що актуалізує тематику цієї наукової статті.

Вивчення феномена правового регулювання штучного інтелекту в Україні належить до малодосліджених в науці адміністративного та інформаційного права. Сьогодні немає підстав стверджувати, що ми маємо науково обґрунтовану концепцію адміністративно-правового механізму реалізації правової доктрини у сфері штучного інтелекту. Виняток становлять роботи, присвячені як загальним, так і окремим проблемам забезпечення використання штучного інтелекту в різних галузях права, що наразі не знімає гостроти порушеної нами проблематики. Окремі її аспекти розглядалися у працях Т.Л. Антонової, К.В. Барсукової, Ю.А. Будника, В.В. Галунька, В.М. Гаращука, Р.А. Калюжного, О.Е. Радутного, О.Й. Розвадовського, Р.А. Сербіна, А.О. Сидоренка, А.О. Собакаря, В.В. Топчія, В.В. Шеховцова, В.Д. Чернія, О.Ш. Чомахашвілі, О.С. Юніна та інших. та ін.

Слід виокремити колективну монографію авторського колективу Інституту проблем штучного інтелекту Міністерства освіти і науки України і Національної академії наук України «Стратегія розвитку штучного інтелекту в Україні» за загальною редакцією А.І. Шевченка, опубліковану в Києві у 2023 році, у якій закладено основи дослідження штучного інтелекту в різних сферах суспільної діяльності; докторську дисертацію з державного управління Т.В. Запорожця «Формування та реалізація механізмів запровадження інтелектуального управління у діяльності органів державної влади», захищену в м. Харків у 2021 році, в якій здійснено теоретико-методологічне обґрунтування та розроблено практичні рекомендації щодо формування та реалізації механізмів запровадження інтелектуального управління у діяльності органів державної влади.

Разом із тим у роботах названих авторів є істотні розбіжності у підходах до самого розуміння поняття штучного інтелекту, не повною мірою розкрито діяльнісний бік функціонування системи органів державної влади, до компетенції яких належить адміністративно-правовий механізм реалізації

правової доктрини у сфері штучного інтелекту. Багато досліджень, незважаючи на високий рівень теоретичних узагальнень, залишило за межами викладу прикладні аспекти значення правового регулювання цієї сфери. Здебільшого жоден із вищезазначених дослідників не робив спроб вивчення впливу основних тенденцій розвитку соціальних процесів на стан правового забезпечення стратегії і тактики використання штучного інтелекту в Україні в умовах захисту від збройної агресії. Проте для розробки концептуальних положень адміністративно-правового механізму реалізації правової доктрини у сфері штучного інтелекту, їх прогнозування, а також вибору ефективних засобів і способів їх упровадження теоретичні дослідження в галузі правознавства, зокрема в адміністративному та інформаційному праві, мають суттєве значення [106].

Вищезазначений комплекс обставин зумовив науковий інтерес до порушеного кола питань, а також їх теоретичне опрацювання на дисертаційному рівні.

Дослідженню проблематики впровадження ШІ у сферу обороноздатності присвятили свої публікації такі вчені як В. Є. Хаустова, О. І. Решетняк, М. М. Хаустов, В. А. Зінченко [61], З. В. Гбур [5], М. О. Кизим, В. В. Шпілєвський, О. В. Шпілєвський [14]. Проте у наведених дослідженнях недостатньо уваги приділено обґрунтуванню проблематики та перспектив упровадження ШІ у сферу забезпечення національної безпеки та обороноздатності України в повоєнний період; розгляду основних нормативно-правових актів, які містять положення про впровадження ШІ; негативним та позитивним рисам запровадження ШІ у вказаному напрямі; питанням трансферу технологій ШІ через сферу забезпечення національної безпеки та обороноздатності в інші галузі економіки [106].

З моменту свого виникнення в середині 1950-х рр. тематиці штучного інтелекту присвячено багато досліджень науковців з усього світу, але саме з 2000 р. спостерігається стрімке зростання досліджень, розробок і практичного застосування ШІ в різних сферах [75; 101; 60; 56]. Так, К.

Шульман (C. Shulman) досліджував накопичувачі ШІ, ймовірність їх співпраці з людьми та ризики, пов’язані зі застосуванням ШІ [99]. Н. Бостром (N. Bostrom) та інші показали, що створення самовдосконалюючого надінтелектуального ШІ є реальною можливістю в найближчі кілька десятиліть, хоча й несе високі ризики практичного використання [56; 99; 83]. Дж. Тетлоу (G. Tetlow) відмічає, що використання ШІ для мілітаристських цілей стає більш привабливим з кожним роком [103]. С. Де Шпиглер, М. Маас і Т. Свейс (S. De Spiegeleire, M. Maas, T. Sweijs) показали, що розвиток технологій ШІ впливає не тільки на вдосконалення високоточного озброєння, а й на розвиток стратегічного планування, підвищує рівень організації всередині військових структур і змінює принципи організації національної оборони в напрямку надрозумного ШІ [87]. Аллен Г. і Чан Т. (G. Allen, T. Chan) проаналізували глобальні катастрофічні ризики ШІ та визначили перспективи злиття в майбутньому цивільної галузі штучного інтелекту й американської системи безпеки [74]. Л. Саалман (L. Saalman) [105] та І. Сабадфолді (I. Szabadföldi) [101] свої дослідження присвятили розгляду можливостей і ризиків ШІ у сфері безпеки загалом, а також сфері застосування ШІ у військовій сфері зокрема.

Проте, незважаючи на велику кількість наукових робіт, присвячених ШІ та його використанню в оборонній сфері, впливу нових технологій ШІ на національну обороноздатність країн світу присвячено недостатньо уваги. Отже, надвисока актуальність даної проблематики та динамічність змін у сфері розвитку ШІ свідчить про необхідність її подальших досліджень.

Дослідження з питань використання штучного інтелекту в Україні відзначаються значним розмаїттям тематичних напрямків та наукових напрацювань авторів у цій сфері знань. Зокрема, вчені досліджують роль і особливості штучного інтелекту в науці та освіті, серед яких І. Візнюк, Л. Філіпенко, Ю. Бисага. І. Голубенко, О. Павлюк, Є. Тимошенко. Про вплив штучного інтелекту на економіку розкрито такими дослідниками, як А. Шрейдер, Б. Дмитрів, Г. Андрощук, М. Бортнікова, Л. Чиркова, В. Кузьомко.

О.В. Цеслів. Про особливості використання штучного інтелекту в інформаційній та кібербезпеці опубліковано наукові праці таких фахівців, як О. Радутний, В. Устименко, І. Олішевський, В. Богом'я, А. Гудзя, С. Лисенко, М. Копійка. Питання використання штучного інтелекту в оборонній сфері висвітлено такими вченими, як В. Хаустова, О. Решетняк, М. Хаустовий, В. Зінченко, З. Гбур. Штучний інтелект в публічному управлінні розкрито у працях таких дослідників, як С. Квітка, Н. Новіченко, О. Бардах, Л. Корнут, Л. Треба. Також проведено дослідження щодо нормативно-правового регулювання штучного інтелекту такими фахівцями, як С. Барабашин, Ю. Кривицький, Д. Позова, Д. Коваленко, М. Уткіна, С. Залєвський. Т. Тарасевич, Я. Свистун тощо.

Зауважимо, що ці дослідження допомагають відкривати нові можливості для впровадження штучного інтелекту в різні сфери життя. Наприклад, дослідження в області науки та освіти можуть сприяти розвитку інноваційних методів навчання та досліджень, що покращить якість освіти та дозволить досягти нових наукових досягнень. Вивчення впливу штучного інтелекту на економіку також є дуже важливим, оскільки він може стати ключовим фактором у зміні бізнес-моделей та створенні нових ринків. Застосування штучного інтелекту в формаційній та кібербезпеці дозволить покращити захист інформації та боротьбу з кіберзлочинами. У сфері оборони штучний інтелект може забезпечити покращення військової стратегії та обладнання для захисту країни. Публічне управління також може отримати значну вигоду від використання штучного інтелекту, що покращує ефективність управлінських рішень та послуг для громадян. Однак використання штучного інтелекту породжує також питання етики та нормативного регулювання. Це потребує поглибленого вивчення та розробки відповідних правил і стандартів. Деякі дослідження вже присвячені цим питанням, але їхній подальший розвиток та вдосконалення є критичними задля забезпечення безпеки та ефективності використання штучного інтелекту.

Висновки до 1-го розділу

Розглянувши питання визначення поняття «штучний інтелект» в різних аспектах, можемо зазначити, що шлях у десятиріччя доволі складний і суперечливий. Так, звичайно є побоювання щодо проведення аналогії з людським інтелектом у буквальному розумінні, що може призвести до хибного визначення. Потрібно враховувати той факт, що до сьогодні неможливо точно визначити та виміряти людський інтелект.

Отже, якщо дослідження штучного інтелекту проводяться останні десятиліття, то осягнути розуміння та можливості людського інтелекту не вдається ще з античних часів, тисячоліття. Проводячи паралель, можемо зазначити, що так само складно і суперечливо буде проходити пізнання штучного інтелекту та його нормативне закріплення.

З моменту свого виникнення в середині 1950-х рр. тематиці штучного інтелекту присвячено багато досліджень науковців з усього світу, але саме з 2000 р. спостерігається стрімке зростання досліджень, розробок і практичного застосування ШІ в різних сферах. Дослідження з питань використання штучного інтелекту в Україні відзначаються значним розмаїттям тематичних напрямків та наукових напрацювань авторів у цій сфері знань.

РОЗДІЛ 2. АДМІНІСТРАТИВНІ ТА НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРНЕТИЧНУ БЕЗПЕКУ ДЕРЖАВИ

2.1. Адміністративні процедури забезпечення впровадження технологій штучного інтелекту в кібернетичну безпеку держави.

Запровадження різноманітних новітніх технологій у повсякденне життя людей та функціонування держави і суспільства потребує нормативного упорядкування діяльності з їх створення та використання, оскільки такі технології можуть спричиняти суттєвий вплив на існуючі суспільні відносини у різних сферах життєдіяльності людини і державних інституцій шляхом їх зміни, ліквідації чи продукування нових. Зазначений вплив чиниться на різні галузі права, зокрема й на адміністративне, що своєю чергою вимагає розробки поняття та з'ясування сутності адміністративного регулювання відповідної сфери.

Повною мірою вищесказане стосується і галузі розвитку такої новітньої технології в Україні, як штучний інтелект.

На сьогодні в Україні штучний інтелект використовується в різноманітних галузях суспільного життя. Його застосування охоплює такі напрямки, як державне управління, місцеве самоврядування, національна та громадська безпека, включаючи інформаційну та кібербезпеку. Штучний інтелект використовується в розвитку смарт-інфраструктури, у сфері житлово-комунального господарства, бізнес-процесах та системах, промисловому виробництві, електроенергетиці, ринку товарів і послуг, включаючи торгівлю, трансфертне ціноутворення, банківську справу з управлінням ризиками, оцінюванням, прогнозуванням і аналітикою, а також використанням чат-ботів у мобільних банківських додатках. Штучний інтелект широко застосовується в транспорті для оптимізації управління автомобільним транспортом, розширення можливостей круїз-контролю та автопілоту, а також у сфері логістики для підвищення продуктивності та

зменшення простоїв. Він знаходить застосування у сфері телекомунікацій, медицини для ведення документації та діагностики, освіти, науки, культури та спорту [11].

Проте не існує жодної галузі державного або суспільного життя, яку не зачіпали б питання адміністративно-правового регулювання [17, с. 193]. Концепція розвитку штучного інтелекту в Україні визначає галузь штучного інтелекту як напрям діяльності у сфері новітніх інформаційних технологій, який забезпечує створення, впровадження та використання технологій штучного інтелекту [19].

Слід відмітити, що у доктрині адміністративного права відсутне визначення адміністративно-правового регулювання зазначеного виду діяльності. А у Концепції розвитку штучного інтелекту в Україні зазначається, що однією з першочергових проблем розвитку технологій штучного інтелекту в Україні є, зокрема, відсутність або недосконаліть правового регулювання публічного управління у цій сфері [19].

Отже, зважаючи на те, що запровадження технологій штучного інтелекту є важливим елементом людської діяльності, який сприяє розвитку суспільства і держави, то правильне з'ясування сутності і змісту поняття адміністративно-правового регулювання такої діяльності, як створення, впровадження та використання штучного інтелекту в Україні, буде слугувати гарною основою для подальшого практичного втілення новітніх технологій в нашій державі та розвитку суспільних відносин у цьому напрямку.

На сьогодні ключовим органом, що уповноважений на здійснення публічного адміністрування діяльності зі створення, впровадження та використання штучного інтелекту в Україні є такий орган виконавчої влади, як Міністерство цифрової трансформації України (Мінцифри).

Мінцифри є «головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної

демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті» [31].

Важливе місце серед суб'єктів публічного адміністрування розгляданого виду діяльності займає також Державне підприємство

«Український інститут інтелектуальної власності» (Укрпатент), оскільки воно виконує функції Національного органу інтелектуальної власності та уповноважене, зокрема, здійснювати державну реєстрацію винаходів і корисних моделей, видавати патенти на винаходи і корисні моделі. За своєю суттю це є діяльністю з надання адміністративних послуг.

Категорія «адміністративна послуга» може розглядатися, зокрема, крізь призму змістового смислу «послуги» у приватно-правовому розумінні як діяльність, що спрямована на задоволення певних потреб особи, яка звернулася за здійсненням послуги» [72, с. 15]. Однією з таких потреб є державна реєстрація новостворених винаходів та корисних моделей, що являють собою і технології штучного інтелекту.

Діяльність із впровадження та використання технологій штучного інтелекту також потребує урегулювання з боку держави. На сьогодні така прерогатива належить тим органам виконавчої влади або органам місцевого самоврядування, які безпосередньо впроваджують технології штучного інтелекту у свою діяльність.

Наприклад, «Київська міська державна адміністрація, громадськість та AI-розробники працюють над розвитком столичної СМАРТ-інфраструктури,

зокрема над впровадженням міських цифрових сервісів на базі штучного інтелекту. Команда проєкту «AI for Kyiv» («Штучний інтелект для Києва») проводить дослідження питання етики та дискримінації в розробках сервісів на базі штучного інтелекту у різних сферах та ініціює дискусію про цифрові права людей в Україні. Розробляються оптимальні рішення для покращення якості життя в столиці на основі принципів відкритого доступу до даних, а також інтелектуальної та прозорої трансформації управління містом із використанням сучасних технологій та інновацій» [23].

Крім цього, на 52 станціях метро в Києві розташовано близько двохсот камер відеоспостереження, обладнаних, серед іншого, системами розпізнавання облич. Епіцентром нових технологій є перехідні, кінцеві та найбільш завантажені станції. Деякі з цих камер також проводять аналіз температури людей, які планують увійти до київського метрополітену. Зібрані дані передаються поліції, муніципальній варті, державній службі з надзвичайних ситуацій, а також використовуються як джерело статистичної інформації для департаменту охорони здоров'я Київської міської державної адміністрації [11]. А «ПриватБанк запустив перші в Україні біометричні платіжні POS-термінали з технологією FacePay24, яка дозволяє оплачувати покупки обличчям. FacePay24 використовує одну з провідних в світі систем штучного інтелекту із автоматичного розпізнавання обличчя Amazon Rekognition та забезпечує повну безпеку персональних даних клієнтів, включаючи технічні і фізичні контролі, шифрування даних при зберіганні і передачі» [33].

Водночас технології штучного інтелекту так само можуть впроваджувати та використовувати у своїй діяльності і приватні структури: банківські установи, великі промислові підприємства, транспортні компанії тощо.

Однак, ключовим питанням залишається легальність впровадження та використання таких систем: «наявність правової бази для їх функціонування в українському законодавстві, умови та необхідність втручання у конкретних

обставинах, передбачуваність втручання для пересічних громадян, а також належні запобіжники від зловживань» [64].

Крім того, фахівці відзначають необхідність у налагодженні співпраці держави з приватним сектором на правах взаємовигідного партнерства шляхом стимулювання інвестицій та ринку стартапів, шляхом надання з державного бюджету та використання місцевими бюджетами міжбюджетних трансфертів на розвиток технологій штучного інтелекту [11]. Ця діяльність також має бути у сфері належно організованого публічного адміністрування з боку держави.

Вищенаведене свідчить, що ефективність розвитку технологій штучного інтелекту у нашій державі потребує єдиного управлінського органу, який би міг централізовано, на державному рівні здійснювати контроль, визначати мету, завдання, цілі, принципи, форми та методи діяльності із розробки, впровадження та використання штучного інтелекту в Україні. У структурі Мінцифри такий орган відсутній. Ним може стати єдиного управлінський орган в Україні – Національне агентство штучного інтелекту (НАШІ).

Хоча висловлена ідея не є новою. Наприклад, автори проєкту Національної стратегії розвитку штучного інтелекту в Україні 2021-2030 наголошують, що «система управління та регулювання штучного інтелекту в Україні повинна забезпечувати стійкий розвиток технологій штучного інтелекту, ефективний контроль над ними. Виконання цих завдань слід покласти на Комітет штучного інтелекту, який пропонується створити» [25]. Натомість О.М. Охотнікова також пропонує «створити державний орган виконавчої влади зі спеціальним статусом – Державний комітет штучного інтелекту, сфера повноважень якого буде виключно спрямована на розвиток нейронних технологій в Україні та їх запровадження в публічне адміністрування земельних відносин» [28, с. 134].

Проте, відповідно до закону України «Про центральні органи виконавчої влади» до переліку таких органів, у першу чергу, входять

міністерства, а також інші центральні органи виконавчої влади: служби, агентства, інспекції, комісії, бюро [40]. Комітети до переліку центральних органів виконавчої влади не входять. Що стосується інших органів, то створення, наприклад, Національного агентства штучного інтелекту, може призвести до того, що його функції та повноваження можуть частково збігатись із функціями та повноваженнями Мінцифри, що варто враховувати при створенні цього агентства.

А О.В. Білокобильський пропонує створити центральний орган виконавчої влади, що здійснюватиме державну політику в сфері штучного інтелекту – Ради з питань безпеки розробок у сфері штучного інтелекту. Цей орган має об'єднати представників основних зацікавлених сторін: Уряду, наукової спільноти, громадянського суспільства, бізнесу та буде підзвітний Прем'єр-міністру України. Ключова мета цього органу – моніторинг розробок у сфері штучного інтелекту на предмет відповідності пріоритетам, визначеним у Стратегії розвитку штучного інтелекту в Україні, а також «Законі про штучний інтелект» та інших нормативних документах, зокрема пріоритету безпеки та етичних норм і принципів [69, с. 98].

Між тим, на сьогодні в Україні реалізується політика щодо скорочення кількості центральних органів влади. Так, КМУ ініціював реформу зменшення кількості державних службовців. Реформа передбачає, зокрема, зміни у кількості міністерств, їх планують зменшити з 20 до 14 [46]. У рамках цього планується масштабне скорочення державного апарату і бюджетників, ліквідація і скорочення різноманітних державних агентств, служб, управлінь та інспекцій. При чому, Мінцифри планується залишити як окреме міністерство з включенням до його структури Міністерства з питань стратегічних галузей промисловості [1]. Тому створення Ради з питань безпеки розробок у сфері штучного інтелекту як окремого центрального органу виконавчої влади виглядає недоречним, його функції матиме загальне агентство.

Зважаючи на вищевикладене існує необхідність у створенні у складі Мінцифри Департаменту з розвитку, впровадження та використання штучного інтелекту, який би здійснював виключно публічне адміністрування діяльності зі створення, впровадження та використання штучного інтелекту в Україні, і при цьому підпорядковувався центральному органу виконавчої влади, який реалізує державну політику у сфері розвитку цифрових технологій – Мінцифри [16].

Департаменту може бути доручено виконання таких завдань, серед яких: координація роботи українських і міжнародних вчених, що працюють в Україні над розробками у сфері штучного інтелекту, створення та розвиток майданчика для об'єднання зусиль і забезпечення синергії; попередня оцінка систем штучного інтелекту, які можуть становити високий ризик для життя громадян та стабільності суспільства, на відповідність принципам та етичним нормам, визначених Стратегією розвитку штучного інтелекту в Україні; ліцензування розробок у сфері штучного інтелекту, які стосуються стратегічно важливих напрямів національного господарства; здійснення періодичного моніторингу впроваджених систем штучного інтелекту, які можуть мати високий ризик для суспільства, протягом їхнього життєвого циклу задля визначення їхнього впливу на суспільство і можливої корекції роботи цих систем; перевірка українських розробок у сфері штучного інтелекту на відповідність європейським стандартам безпеки та захисту даних, приватності, прозорості тощо; співпраця з європейськими та іншими міжнародними регуляторами розробок у сфері штучного інтелекту; підготовка пропозицій щодо внесення змін до чинних нормативних актів або прийняття нових законодавчих актів у сфері штучного інтелекту з урахуванням постійного розвитку та змін у функціоналі систем штучного інтелекту; моніторинг діяльності органів виконавчої влади щодо впровадження Стратегії розвитку штучного інтелекту в Україні та підготовка пропозицій стосовно вдосконалення процесу імплементації; організація навчальних заходів для державних посадовців, які працюють з системами

штучного інтелекту, та координація впровадження освітніх програм у сфері штучного інтелекту в українських освітні заклади; організація заходів для підвищення обізнаності громадян України стосовно новітніх розробок у сфері штучного інтелекту, а також сприяння підвищенню довіри до таких розробок завдяки впровадженню прозорих стандартів безпеки [69, с. 98-99].

У Концепції розвитку штучного інтелекту в Україні зазначається, що її метою є «визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб, побудови конкурентоспроможної національної економіки, вдосконалення системи публічного управління» [19]. А у проєкті національної Стратегії розвитку штучного інтелекту в Україні у якості мети цієї стратегії зазначається, що вона повинна забезпечити «передумови стійкого економічного розвитку держави та відповідно зростання добробуту і якості життя її населення, виведення України на провідні позиції у світі в галузі інформаційних і комп'ютерних технологій шляхом ефективного використання переваг і можливостей широкого впровадження штучного інтелекту в усі сфери суспільного життя» [25].

Завдання будь-якого виду адміністративно регулювання конкретизують мету відповідного регулювання, а також основні етапи його здійснення [65]. Вони являють собою наперед визначений, запланований до виконання обсяг робіт, покладений на суб'єкта публічного адміністрування. Відповідно перед кожним суб'єктом ставиться чітко визначене коло завдань [2, с. 67].

Так, основними завданнями Мінцифри, відповідно до Положення про Міністерство цифрової трансформації України від 18 вересня 2019 р. є «формування та реалізація державної політики:

– у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства;

– у сфері розвитку цифрових навичок та цифрових прав громадян;

– у сферах відкритих даних, розвитку національних електронних

інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу;

– у сфері надання електронних та адміністративних послуг;

– у сферах електронних довірчих послуг та електронної ідентифікації;

– у сфері розвитку ІТ-індустрії» [31].

Слід відмітити, що у переліку вищенаведених головних завдань, що КМУ поставив перед Мінцифри, відсутнє чітке та конкретне завдання, пов'язане з публічним адмініструванням діяльності із впровадження технологій штучного інтелекту в Україні.

Хоча серед двадцяти семи напрямків діяльності, що уповноважене здійснювати Мінцифри, відповідно до покладених на нього головних завдань, є забезпечення розвитку штучного інтелекту (абз.3 п.п.14 п.4 Положення про Міністерство цифрової трансформації України [31]). Водночас розвиток технологій штучного інтелекту має бути не просто одним із багатьох напрямків діяльності, а одним із головних, пріоритетних завдань Мінцифри. Це обумовлено тим, що саме штучний інтелект є однією з найбільш передових та складних технологій, а тому питання публічного адміністрування відповідної діяльності мають потребувати особливо пильної уваги з боку уповноважених на те органів. При чому, публічне адміністрування має стосуватись не просто розвитку, а саме таких видів діяльності, як створення, впровадження та використання технологій штучного інтелекту, як це зазначено у Концепції розвитку штучного інтелекту в Україні.

Мінцифри здійснює регулятивну функцію при упорядкуванні суспільних відносин у галузі розвитку технологій штучного інтелекту, що виникають у зв'язку з їх створенням, впровадженням та використанням. Ця функція є важливою для будь-якого виду адміністративно-правового регулювання зважаючи на вжиття власне терміну «регулювання» у

розгляданій категорії адміністративного права.

Використовуючи цю функцію Мінцифри та Укрпатент застосовують різноманітні засоби і механізми адміністративно-правового регулювання діяльності зі створення, впровадження та використання штучного інтелекту, що за своїм змістом є господарською діяльністю. Згідно зі ст. 12 Господарського кодексу України такими засобами регулюючого впливу держави на діяльність суб'єктів, що здійснюють створення, впровадження та використання технологій штучного інтелекту, будучи при цьому суб'єктами господарювання, виступають: «державне замовлення; ліцензування, патентування і квотування; технічне регулювання; застосування нормативів та лімітів; регулювання цін і тарифів; державне замовлення; надання інвестиційних, податкових та інших пільг; надання дотацій, компенсацій, цільових інновацій та субсидій» [7].

У проєкті національної Стратегії розвитку штучного інтелекту в Україні 2021-2030 зазначається, що «система управління та регулювання штучного інтелекту в Україні повинна забезпечувати стійкий розвиток технологій штучного інтелекту, ефективний контроль над ними і має ґрунтуватися на базових етичних нормах і принципах:

– пріоритет добробуту людини (мета забезпечення добробуту людини повинна переважати над іншими цілями розробки та застосування систем штучного інтелекту);

– заборона на заподіяння шкоди за ініціативою систем штучного інтелекту (за загальним правилом слід обмежувати розробку та застосування системи штучного інтелекту, здатних за своєю ініціативою цілеспрямовано заподіювати будь яку шкоду людині);

– підконтрольність людині (тою мірою, якою це можливо з урахуванням необхідного ступеня автономності систем штучного інтелекту);

– проєктована відповідність законам (застосування систем штучного інтелекту не повинно свідомо для розробника призводити до порушення правових норм);

– недопущення прихованої маніпуляції поведінкою людини;

– проєктована безпека (при розробці систем штучного інтелекту повинен забезпечуватися достатній рівень особистої та громадської безпеки)» [25].

Крім того, у проєкті національної Стратегії розвитку штучного інтелекту в Україні зазначається, що «наша держава повинна мати власну стратегію розвитку штучного інтелекту, яка б регламентувала відповідні дослідження та розробки, підготовку необхідної кількості фахівців з визначеними компетенціями, обсяг і напрями фінансування галузі, формування керівних і наглядових органів для регулювання впровадження імпортованих технологій, етичного контролю тощо» [25].

Отже, на сьогодні є першочергова потреба у прийнятті Національної стратегії розвитку штучного інтелекту в Україні.

Можуть виникнути питання щодо доцільності прийняття стратегії, якщо вже прийнято концепцію. Проте, «концепції виражають лише розуміння певної проблеми і не є керівництвом до дії, а стратегії передбачають більш глибоке осмислення об’єкта розробки, ніж концепції, і завжди зорієнтовані на досягнення конкретної мети» [71].

Таким чином, адміністративне регулювання діяльності зі створення, впровадження та використання штучного інтелекту в Україні потребує розробки та прийняття необхідної адміністративної системи, до якої, у першу чергу, має належати закон України «Про правовий статус штучного інтелекту та загальні засади створення, впровадження та використання його технологій в Україні».

Також слід враховувати, що «впровадження технологій штучного інтелекту має відбуватись у багатьох галузях суспільного життя в Україні, а саме в: промисловості, економіці, транспорті та інфраструктурі, науковій діяльності, медицині, сільському господарстві, екології, оборонній промисловості тощо» [71].

У Концепції розвитку штучного інтелекту в Україні визначено пріоритетні сфери, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, є: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя.

2.2. Нормативно-правові засади впровадження технологій штучного інтелекту в кібернетичну безпеку держави.

Усталена безпека – одне з наріжних питань, яке поставало перед Україною впродовж її багатовікової історії. Повномасштабна збройна агресія РФ проти України оголила численні загрози, що виникли не тільки перед нашою державою, а й перед всією світовою системою безпеки в цілому.

Забезпечення національної безпеки та обороноздатності України в повоєнний період має стати головним пріоритетом військово-політичного керівництва держави.

Досвід зарубіжних країн доводить, що швидке, ефективне та гнучке забезпечення потреб суспільства у воєнній безпеці та обороноздатності держави в повоєнний період досягається шляхом упровадження новітніх технологій, зокрема застосування ШІ та Big Data, як пріоритету подальшого розвитку оборонно-промислового комплексу повоєнної України. На сьогодні ШІ належить до таких технологічних сфер суспільного розвитку, які стрімко розвиваються та мають великий потенціал у багатьох галузях, включаючи національну безпеку, оборону, військову медицину, військову логістику, розвідку і контррозвідку, аеророзвідку тощо. Вказане пояснює суть обраної проблематики, актуальність і потребу в її дослідженні.

Оборонно-промисловий комплекс (ОПК) стратегічно був, є і повинен стати джерелом запровадження новітніх технологій, у тому числі окремих інформаційно-комунікаційних технологій. Виникнення, розвиток та стрімке поширення ІКТ, зокрема ШІ, надають поштовх інноваційним перетворенням

ОПК і стають драйвером перетворень інших галузей економіки через інструмент трансферу технологій у різних країнах світу.

Підтвердженням важливості використання ШІ для забезпечення національної безпеки є результати досліджень Науково-технічної організації НАТО, що визначають найбільш суттєві з них для розвитку технологій, згідно з якими ключовими технологіями є ШІ, Big Data, автономні транспортні засоби, космос, гіперзвукові літальні апарати, квантові технології, біотехнології, нові матеріали тощо [61, с. 18].

Вказане повністю вкладається в концепт «Четверта промислова революція», який обґрунтовує, що драйверами розвитку світової економіки є інноваційні технології, які не лише кардинально змінюють усі галузі економіки, у тому числі ОПК, з метою забезпечення національної безпеки та обороноздатності, а й створюють абсолютно нові типи виробництва, які базуються на аналізі ШІ, Big Data, роботизації, доповненій реальності, Інтернеті речей (Internet thing) тощо. Фактично Індустрія 4.0 – це всі сфери життєдіяльності суспільства, на які можуть біти поширені новітні технології [63, с. 7].

З аналізу щорічних доповідей Стенфордського університету «Artificial Intelligence Index Report» відомо, що протягом останніх років багато держав розробили довгострокові національні Стратегії розвитку ШІ та здійснюють певні заходи щодо їх упровадження.

У цілому стратегії розвитку ШІ різних країн світу науковці поділяють на три основні групи: а) група, яка визначається реалістичним ставленням до формування стратегій ШІ, глибоким аналізом не тільки стану сфери застосування ШІ в країні, а й дійсних потреб її розвитку. Стратегії країн цієї групи мають фундаментальний характер і відображають як загальні світові проблеми впровадження ШІ, так і конкретні плани реінжинірингу різноманітних секторів ринку та бізнесу, цифровізації багатьох галузей національних економік та різних сфер суспільних відносин (Королівство Саудівська Аравія, США тощо); в) група країн, для яких характерним є

ґрунтовний і прагматичний підхід до цілей та етапів їх досягнення з урахуванням дійсних потреб держави і формування окремих унікальних завдань та цілей розвитку ШІ (Велике Герцогство Люксембург, Республіка Мальта, Малайзія, Республіка Литва); с) група країн, стратегії яких виконані у формалізованому вигляді, налічують базові цілі розвитку країни в напрямі впровадження технологій зі ШІ в певних сферах суспільної життєдіяльності (Австралія, Республіка Австрія, Королівство Іспанія, Держава Катар, Португальська Республіка, Республіка Кіпр, Нова Зеландія, Держава Ізраїль, Швейцарська Конфедерація тощо) [20, с. 59−60].

Прагматичне питання, що виникає у зв'язку з викладеним вище: чи сформовано Україною стратегічне бачення використання можливостей ШІ у сфері забезпечення національної безпеки та обороноздатності в контексті інтеграції в концепт «Індустрія 4.0»?

Наразі Україною прийнято шість програмних довгострокових документів у безпековому напрямі, які стосуються (прямо або опосередковано) питань національної безпеки та обороноздатності держави і торкаються проблематики використання ШІ, Big Data та сучасних ІКТ у вказаних сферах: 1) Стратегія забезпечення державної безпеки [37], якою передбачено, що основними завданнями державної політики у сфері забезпечення державної безпеки є завершення створення, подальший розвиток і посилення спроможності національної системи кібербезпеки, оптимізація координації її суб'єктів з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі; створення ефективної системи обміну інформацією між суб'єктами забезпечення державної безпеки та запровадження дієвих механізмів доступу суб'єктів забезпечення державної безпеки до державних електронних інформаційних ресурсів та автоматизованих інформаційних і довідкових систем, реєстрів, банків (баз) даних; 2) Стратегія національної безпеки України [48], згідно з якою: 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 ШІ, які докорінно трансформують економіку і суспільство в цілому; розробляються системи озброєнь на основі нових фізичних принципів із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері ШІ, створення нових матеріалів, робототехніки та автономних безпілотних апаратів; основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації; Україна зміцнить бойовий потенціал Збройних Сил України, інших органів сил оборони шляхом: удосконалення та розвитку на основі сучасних технологій систем управління, телекомунікацій, розвідки, логістики; 3) Стратегія інформаційної безпеки [38], яка передбачає, що основними напрямами забезпечення інформаційної безпеки України є протидія дезінформації та інформаційним операціям, насамперед держави-агресора. Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань: створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі; 4) Стратегія кібербезпеки України [39], якою передбачено, що забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Розширення кола держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет, вказує на потребу в забезпеченні національної безпеки та обороноздатності України. Швидко змінюваний цифровий світ вимагає формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового

середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачаючи нові можливості для цифровізації всіх сфер суспільного життя; 5) Стратегія воєнної безпеки України [36], відповідно до якої на глобальному рівні основними аспектами воєнної безпеки є руйнування створеної після Другої світової війни системи міжнародної безпеки, підвищення рівня невизначеності та непередбачуваності безпекового середовища, яке характеризується, зокрема, конкуренцією держав у сфері космічних, квантових, інформаційних, кібернетичних, гіперзвукових, біологічних, нанота інших технологій, розробленням на їх основі систем озброєнь з використанням нових фізичних принципів, робототехніки та новітніх матеріалів, мілітаризацією навколоземного космічного простору. Визначені пріоритети можуть бути реалізовані шляхом виконання таких основних завдань: розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохопної оборони України; підвищення рівня боєздатності Збройних сил України та інших складових сил оборони з досягненням і підтриманням визначених спроможностей щодо вогневого ураження противника, застосування авіації та протиповітряної оборони України, контролю ближньої морської зони, ведення спеціальних операцій, територіальної оборони України, управління та всебічного забезпечення військ (сил), відбиття агресії в кіберпросторі (ведення кібероборони); 6) Стратегія розвитку оборонно-промислового комплексу України [49], згідно з якою створення умов для розвитку ОПК України здійснюється з використанням механізмів державно-приватного партнерства та військово-технічного співробітництва з іноземними державами для виробництва високоефективного озброєння, військової та спеціальної техніки для задоволення потреб Збройних сил України, інших органів сектору безпеки і оборони, збільшення експортного потенціалу оборонно-промислового комплексу України і є метою державної військово-промислової політики. Світовими тенденціями розвитку ОПК є, зокрема,

високі темпи технологічних змін і перехід до нового технологічного укладу (штучний інтелект, розвиток нових технологій зв'язку, біотехнологій, електроніки тощо) ведуть до появи нових і скорочення старих ринків, серед виробників озброєнь загострюється конкуренція. Тенденціями розвитку озброєнь є те, що провідні держави світу здійснюють активні заходи з переозброєння своїх військ. Зміни способів ведення збройної боротьби формують нові потреби у розробленні озброєнь на основі нових фізичних принципів з використанням квантових, інформаційних, космічних, гіперзвукових технологій, біотехнологій, а також технологій у сфері штучного інтелекту, створюються нові матеріали, робототехніка та автономні безпілотні апарати, удосконалюються неядерні високоточні озброєння [18].

Окрім того, Кабінет Міністрів України розпорядженням від 12 травня 2021 року № 438-р затвердив План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки [34], згідно з яким на вказаний період передбачено низку заходів та законодавчих ініціатив, зокрема запровадження правового регулювання з питань формування державної політики у галузі ШІ; запровадження державної підтримки використання технологій ШІ в пріоритетних галузях економіки; упровадження технологій ШІ в національну систему кібербезпеки для проведення аналізу і класифікації загроз та вибору стратегії їх стримування і запобігання їх виникненню; визначення пріоритетних напрямів і основних завдань розвитку технологій ШІ в документах оборонного планування тощо.

Необхідно зазначити, що 23 лютого 2023 року Верховна Рада України ратифікувала Угоду між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027) [54], метою якої є зміцнення та просування потенціалу Європи в ключових сферах цифрових технологій. Документ створює передумови для участі України в програмі ЄС, яка надає додаткові стимули і можливості для цифрової трансформації пріоритетних галузей і сфер суспільного життя,

розвитку цифрової економіки, ІТ-бізнесу, ШІ та підвищення рівня цифрових навичок громадян.

Отже, можемо констатувати, що європейський напрям цифровізації суспільства та розвитку і поширення ШІ підтриманий Україною на законодавчому рівні.

Наведене вище в цілому доводить, що в Україні сформовано бачення напряму розвитку спеціального законодавства застосування технологій ШІ на основі існуючих оборонних та безпекових потреб. Проте цілісний стратегічний документ, як-то Стратегія розвитку ШІ у сфері забезпечення національної безпеки та обороноздатності України, відсутній, обговорення не відбувається навіть на рівні проекту. Вказане можна визначити як правову лакуну, яка потребує негайного усунення.

Зазначене обумовлює підвищення наукового інтересу і наукових дискусій до впровадження технологій ШІ у сферу забезпечення національної безпеки та обороноздатності України в повоєнний період, напрямів їх застосування, впливу технологій ШІ на ОПК та забезпечення обороноздатності країн світу [61, с. 66−67] і трансферу технологій ШІ через оборонну та безпекову сфери в інші галузі економіки.

Науковці вказують, що розроблення правового регулювання застосування технологій ШІ наразі відбувається вкрай повільно стосовно стрімкого розвитку технологій ШІ, які одночасно охоплюють усі сфери суспільних відносин. Тому контроль за створенням та використанням ШІ необхідно здійснювати не тільки суто технічним регулюванням (вимоги, технічні стандарти, регламенти, оцінки відповідності технічним стандартам, контроль відповідності вимогам технічних регламентів, етичних стандартів), а й шляхом формування комплексного законодавства [20, с. 66−67].

Зрозуміло, що триваюча російська військова агресія змушує по-новому осмислити місію і завдання національного ОПК у повоєнний період. Відтворення тенденцій розвитку озброєнь стандартів НАТО в ОПК України має визначити концептуально нові засади розвитку оборонних технологій,

зростання конкурентоспроможності озброєнь українського виробництва, посилить обороноздатність і національну безпеку, сприятиме економічному зростанню країни [14, с. 36].

Утім, поточна ситуація призвела до усвідомлення необхідності перегляду як існуючих (оперативних і тактичних) підходів до організації економіки воєнного часу, так і загальних (стратегічних) принципів подальшого повоєнного розвитку економіки України за умов наявності потенційної майбутньої загрози [21].

Прикладом успішного застосування такого стратегічного підходу є досвід Ізраїлю, де ОПК відіграє вагому роль у розвитку Армії оборони Ізраїлю (АОІ) та інноваційної економіки країни в цілому. Сутність підходу полягає в тому, що бюджетні на інші видатки Ізраїлю, які спрямовуються у наукові дослідження, підготовку кадрів, військову медицину та інші напрями інноваційного розвитку АОІ, ОПК та сфери безпеки, переносяться в суспільне життя у вигляді будівельних, інформаційно-комунікаційних, промислових, медичних технологій тощо. Тобто активно застосовуються принципи конверсії та трансферу технологій [15, с. 96−97].

На підставі узагальнених даних, які збирались та акумулювались за допомогою сигнального, візуального, людського та інших видів інтелектів, наприклад, для АОІ було розроблено відповідні рекомендації. Завдяки цим рекомендаціям та програмам «Алхімік», «Євангеліє» і «Відділ мудрості» АОІ у травні 2021 року під час боїв у секторі Газа завдано інтенсивних точкових ударів по об’єктах ХАМАС і палестинського Ісламського джихаду, знищено значну кількість бойовиків. Успішне застосування ШІ в секторі Газа та наявні перспективи використання досвіду Ізраїлю в Україні дають підстави сподіватися на принципову зміну тактики ведення воєнних дій і забезпечення новітнім озброєнням українських військ у повоєнний період [5, с. 54−55].

У дослідженні «Штучний інтелект і національна безпека», здійсненому для конгресу США у 2019 році, стверджується, що головною причиною створення різних систем військового призначення, що володіють ШІ, є

необхідність оперативного опрацювання структурованих і неструктурованих даних значних обсягів інформації (так званих великих даних), обумовлена постійним розширенням числа, номенклатури та технічних можливостей сучасних засобів добування інформації. За висновками фахівців, подібні системи найбільш корисні в розвідці, а також під час ідентифікації об'єктів у процесі обробки відео та фотоматеріалів, отриманих із засобів видовий розвідки, наприклад, зображень літальних апаратів, кораблів, різних видів зброї, фізичних осіб тощо, зроблених під різними кутами, освітленням і в різному оточенні. Основним напрямом розвитку військових систем, які мають ШІ, є централізоване планування і координація проведення військових операцій різного масштабу в повітряному, космічному, кібер, морському і наземному просторі. Традиційно технології ШІ широко застосовуються в автономних бойових і мобільних засобах, здатних діяти самостійно і продовжувати виконання завдання (або повертатися на задану позицію) в разі втрати зв'язку з центром управління. Відомими прикладами такої техніки є безпілотні літальні апарати (БПЛА), автономні наземні машини, надводні та підводні апарати різного призначення тощо [5, с. 56].

Отже, світовий досвід запровадження ШІ у сферу національної безпеки та обороноздатності вказує на те, що на сьогодні жодний збройний конфлікт не може бути вирішений без використання новітніх видів озброєння та військових дій, заснованих на інформації, отриманої в ході ідентифікації об'єктів і цілей засобами сучасного обладнання розвідки [5, с. 54], і характеризується трансфером технологій ШІ через оборонну та безпекову сфери в інші галузі економіки.

Наведене вище вказує напрям формування перспективного національного законодавства в частині застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період та доводить ефективність застосування ШІ в ході збройних конфліктів різної локалізації.

Проте слід окремо наголосити, що, як і будь-яке явище реальної дійсності буття, тотальне застосування ШІ не позбавлене негативних рис. Вказана теза породжує питання: чи має прогресуюча перспектива застосування ШІ у сфері забезпечення національної безпеки та обороноздатності негативні наслідки? [24]

Фахівці наголошують, що не треба ігнорувати можливі побічні ефекти застосування ШІ у сфері забезпечення національної безпеки та обороноздатності. Оскільки значення ШІ у цій галузі визначається саме високою швидкістю обробки великих масивів різнорідних даних, що дає змогу істотно скорочувати тривалість циклу управління військами і зброєю, то зворотною реакцією на такий процес може виявитися катастрофічне погіршення ситуації у разі прийняття рішень за неповними, неправильними, сфальсифікованими вихідними даними [5, с. 57].

Отже, світовий досвід застосування ШІ у сфері забезпечення національної безпеки та обороноздатності та безпосередньо у воєнних конфліктах потребує критичного підходу. Варто враховувати і визнані США обмеження щодо застосування ШІ у воєнних діях. Так, на початку 2020 року Міністерство оборони США, розуміючи можливі негативні наслідки дії «розумної» зброї, сформулювало п’ять етичних принципів використання систем ШІ у військових цілях:

1) відповідальність: військовий персонал повинен з належною увагою оцінювати дії ШІ, залишаючись повністю відповідальним за розроблення, розгортання і використання систем ШІ;

2) неупередженість: Міністерство оборони США має робити кроки для мінімізації небажаних відхилень у можливостях систем ШІ;

3) відстеження: військові системи ШІ та їх можливості повинні розроблятися і розвиватися таким чином, щоб персонал мав належний рівень розуміння технології, процесів розроблення та методів застосування. Для військового персоналу повинні бути доступні методології, дані й документація, що належать до використовуваних систем ШІ;

4) надійність: можливості військових систем ШІ повинні бути однозначними, чітко сформульованими. Безпека та ефективність таких можливостей повинні перевірятися випробуваннями та підтверджуватися протягом усього терміну служби;

5) підпорядкування: військові системи ШІ повинні повністю виконувати призначені для них завдання, проте військові повинні мати можливість виявляти та запобігати небажаним наслідкам використання ШІ. Військові також повинні мати можливість виводити з бою або вимикати системи ШІ, у яких були помічені відхилення в роботі [5, с. 59].

На переконання керівництва Об'єднаного центру штучного інтелекту США, американські військові не будуть оснащувати системами ШІ центри управління стратегічним озброєнням, адже за запуски балістичних ракет повинні завжди відповідати тільки люди, тобто рішення про застосування зброї масового ураження має бути прерогативою виключно людини [5, с. 60].

Однак застосування технологій ШІ у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період може допомогти в аналізуванні величезної кількості розвідданих з відкритим вихідним кодом, що виходить з нашої країни. Що ж до очікувань стосовно ШІ у військовому застосуванні протягом наступних десятиліть, то деякі його методи та технології визначать ключові передові військові технології. Так, важливість використання ШІ підкреслюється у звіті «Science & Technology Trends 2020–2040» Організації НАТО з науки та технологій під час формування стратегічних пріоритетів у сфері розвитку озброєння та прийняття політичних рішень для країн НАТО і для країн-партнерів. У звіті вказано, що до 2040 року очікується, що основними характеристиками, які будуть визначати більшість ключових передових військових технологій, будуть такі: інтелектуальність – використання інтегрованого ШІ, орієнтованого на знання аналітичних можливостей і симбіотичного ШІ людського інтелекту для забезпечення застосувань проривних технологій; взаємопов'язаність – експлуатація мережі віртуальних і фізичних доменів, включно з мережами

датчиків, організацій, окремих осіб та автономних агентів, пов’язаних за допомогою нових методів шифрування та технологій розподіленого обліку; поширеність – використання децентралізованого та широкомасштабного зондування, зберігання й обчислення для досягнення нових руйнівних військових ефектів; цифровізація – цифрове поєднання людських, матеріальних та інформаційних областей для підтримки нових руйнівних ефектів [61, с. 19].

Таким чином, більшість напрямів технологічного розвитку військового потенціалу та обороноздатності пов’язані з розвитком ШІ. Цей вплив відбуватиметься переважно завдяки використанню вбудованого ШІ в інші супутні технології, такі як віртуальна/доповнена реальність; квантові обчислення; автономність, моделювання; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних. Штучний інтелект матиме трансформаційний вплив на ядерні, аерокосмічні, кібернетичні технології, технології розробки нових матеріалів та біотехнології. Практики зазначають, що ці наслідки матимуть такий самий стратегічний вплив на зміну у військових технологіях, що й упровадження ядерної зброї [61, с. 22]. У якості проміжного висновку слід зазначити, що ШІ може бути використаний для створення систем розвідки та контролю, які можуть виявляти загрози національній безпеці та вживати заходів для їх запобігання. Він також може бути застосований для автоматизації та оптимізації військових операцій, що дає змогу зменшити ризики для життя військових та підвищити ефективність дій, у військовій логістиці, військовій медицині, аєророзвідці, у використанні БПЛА тощо. Однак, разом з перевагами, ШІ може становити загрозу національній безпеці. Наприклад, країна-агресор може використовувати ШІ для здійснення кібератак та інших злочинів, що можуть негативно впливати на національну безпеку. Також існує ризик, що інші держави можуть використовувати ШІ для проведення кібершпигунства та кібератак на інфраструктуру країни [41].

У лютому 2023 року в Гаазі відбулася перша міжнародна конференція з відповідального використання ШІ у військовій сфері REAIM 23, скликана за ініціативою Нідерландів і Південної Кореї, за участю понад 60 країн. За підсумками саміту його учасники (за винятком Ізраїлю) підписали петицію про те, що країни, які вони представляють, висловлюють прихильність використанню ШІ відповідно до міжнародного права, не підриваючи принципів «міжнародної безпеки, стабільності та підконтрольності».

Серед питань, які також обговорили учасники REAIM 23, надійність військового ШІ, ненавмисні наслідки його використання, ризики ескалації та ступінь залученості людей до процесу ухвалення рішень. На думку критично налаштованих експертів, ця петиція, будучи необов'язковою до виконання, не розв'язує багатьох проблем, включно з використанням ШІ у воєнних конфліктах, а також БПЛА під управлінням ШІ тощо. І такі побоювання далеко не безпідставні. Так, один із найбільших військових підрядників США Lockheed Martin повідомив про те, що його новий навчальний винищувач, перебуваючи в повітрі приблизно 20 годин, увесь цей час керувався ШІ. А гендиректор Google Ерік Шмідт поділився своїми побоюваннями з приводу того, що ШІ може сам спровокувати воєнні конфлікти, зокрема із застосуванням ядерної зброї [32].

Вказане дає нам змогу виокремити позитивні та негативні аспекти застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України у повоєнний період.

Позитивними аспектами варто вважати, зокрема: підвищення ефективності: ШІ може допомогти в зборі та аналізі великих обсягів даних, що забезпечує більш швидкий та точний аналіз інформації, скорочуючи час, необхідний для прийняття рішення; мінімізація ризиків: застосування ШІ може допомогти у попередженні катастроф та мінімізації ризиків для військового персоналу, що забезпечує безпеку та захист держави; забезпечення безпеки: ШІ може бути використаний для забезпечення безпеки країни, а саме, для забезпечення контролю над в'їздом та виїздом на кордоні,

для виявлення та запобігання терористичним актам і злочинам; автоматизація процесів: ШІ може допомогти в автоматизації багатьох процесів у сфері оборони, що зменшує ризик помилок та підвищує ефективність; удосконалення озброєння: ШІ може бути використаний для розроблення та вдосконалення зброї, що забезпечує перевагу військам на полі бою.

Негативні аспекти використання ШІ у сфері забезпечення національної безпеки та обороноздатності України обумовлені таким: етичні проблеми: використання ШІ може порушувати етичні принципи та права людини, зокрема щодо конфіденційності особистих даних та використання зброї; ризики безпеки: використання автономної зброї, керованої ШІ, може створити ризики для безпеки і стати причиною аварій та непередбачуваних наслідків; вразливість систем: ШІ може стати мішенню для кібератак та вірусів, що може призвести до порушення діяльності та непередбачуваних наслідків; залежність від технології: застосування ШІ в забезпеченні обороноздатності може призвести до залежності від технології, що може стати проблемою в разі відмови техніки та відключення від мережі; вартість: використання ШІ в забезпеченні обороноздатності може мати дуже високу вартість та потребувати значних інвестицій у науково-дослідну роботу та розробку технологій.

Узагальнюючи, можна сказати, що для забезпечення національної безпеки та обороноздатності України у повоєнний період необхідно розробляти та впроваджувати у національне законодавство найкращі світові практики, що враховують потенційні можливості та загрози ШІ і забезпечують трансфер технологій ШІ через оборонну та безпекову сфери в інші галузі економіки. Необхідно забезпечити належний рівень кібербезпеки, захистити критичну інфраструктуру та розробити відповідні алгоритми та процедури для виявлення і запобігання загрозам.

Штучний інтелект може стати важливим інструментом у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період, допомагаючи збільшити ефективність та швидкість виконання

військових завдань, знизити ризик втрат, підвищити захищеність військових систем та зменшити витрати на оборону. Однак у ході розроблення та використання ШІ необхідно дотримуватися відповідних правових та етичних стандартів.

Висновки до 2-го розділу

Правильне з'ясування сутності і змісту поняття адміністративно-правового регулювання такої діяльності, як створення, впровадження та використання штучного інтелекту в Україні, буде слугувати гарною основою для подальшого практичного втілення новітніх технологій в нашій державі та розвитку суспільних відносин у цьому напрямку.

Ефективність розвитку технологій штучного інтелекту у нашій державі потребує єдиного управлінського органу, який би міг централізовано, на державному рівні здійснювати контроль, визначати мету, завдання, цілі, принципи, форми та методи діяльності із розробки, впровадження та використання штучного інтелекту в Україні. У структурі Мінцифри такий орган відсутній.

Відповідно існує необхідність у створенні у складі Мінцифри Департаменту з розвитку, впровадження та використання штучного інтелекту, який би здійснював виключно публічне адміністрування діяльності зі створення, впровадження та використання штучного інтелекту в Україні, і при цьому підпорядковувався центральному органу виконавчої влади, який реалізує державну політику у сфері розвитку цифрових технологій.

Розвиток технологій штучного інтелекту має бути не просто одним із багатьох напрямків діяльності, а одним із головних, пріоритетних завдань Мінцифри. Це обумовлено тим, що саме штучний інтелект є однією з найбільш передових та складних технологій, а тому питання публічного адміністрування відповідної діяльності мають потребувати особливо пильної уваги з боку уповноважених на те органів. При чому, публічне

адміністрування має стосуватись не просто розвитку, а саме таких видів діяльності, як створення, впровадження та використання технологій штучного інтелекту, як це зазначено у Концепції розвитку штучного інтелекту в Україні.

Для покращення нормативної бази адміністративно-правового регулювання розглядуваного виду діяльності слід Положення про Міністерство цифрової трансформації України доповнити завданням для Мінцифри, що має полягати у формуванні та реалізації цим міністерством державної політики у сфері створення, впровадження та використання технологій штучного інтелекту в Україні.

Також існує потреба у розробці та прийнятті постанов КМУ про функціонування штучного інтелекту в публічному адмініструванні суспільних відносин різних сферах суспільного життя: будівництва, господарської діяльності, державного управління, енергетики, місцевого самоврядування, медицини, надання адміністративних послуг, науки і освіти, національної безпеки та оборони, правоохоронної діяльності, промислового виробництва, сільського господарства, спорту, транспорту, фінансових послуг тощо. Доцільно передбачити заборону на впровадження та використання таких технологій штучного інтелекту, що здатні спричинити шкоду будь-якій людині з ініціативи таких технологій.

РОЗДІЛ 3. СПЕЦИФІКА ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

3.1. Особливості використання штучного інтелекту у питаннях забезпечення кібернетичного захисту країни.

Динамічний розвиток сучасних передових технологій, зростаюча суцільна залежність від Інтернету провокують постійний ризик появи нових кіберзагроз. В сучасних умовах актуалізується проблематика поширення та впровадження у сфери життєдіяльності людства ноу-хау – інноваційних технологій штучного інтелекту. ШІ стає однією із важливих технологій, поява яких вже змінила чимало сфер людського життя. У сфері комп'ютерних наук ШІ означає здатність машин виконувати завдання, для яких, зазвичай, вимагається наявність людського інтелекту. Сюди відносяться такі завдання, як розпізнавання мови, вирішення технологічних проблем та схвалення оперативних рішень. Аналізуючи великі обсяги інформації та даних, алгоритми ШІ можуть розпізнавати закономірності, з'ясування яких дасть їм змогу згодом покращувати свою роботу. Існують різні види ШІ, кожен з яких володіє унікальними властивостями та обмеженнями, які засвідчують його у якості інноваційної технології [88].

Штучний інтелект – це швидкозростаюча сфера публічного інтересу та інвестицій, яка все активніше використовується для покращення аналізу, прогнозування та захисту від кіберзагроз. Завдяки технологіям ШІ стає можливим відстежувати кіберзагрози, моніторити, прогнозувати й моделювати ситуацію у кіберпросторі, вчасно реагувати на кіберінциденти. На фоні динамічного розвитку інноваційних технологічних рішень, ШІ досить широко застосовується для посилення кібербезпеки, виявлення та ліквідації загроз, посиленого захисту від кібератак, сприяє прийняттю виважених та скоординованих управлінських рішень. У відповідь на зростаючу стурбованість світової спільноти у цій площині, останнім часом, саме технології ШІ відіграють дедалі більш важливішу роль у питаннях

посилення захисту цифрового світу, зокрема, персональних даних, забезпечення кібербезпеки. Загальноприйнятою у світі є позиція про те, що ШІ у сфері кібербезпеки стає дедалі більш важливою складовою останньої у міру розвитку глобального цифрового ландшафту. Розширюючи інструментарій та можливості виявлення й запобігання кіберзагрозам, автоматизуючи рутинні завдання та значно скорочуючи час для реагування на кіберінциденти, технології ШІ допомагають захиститися від кібератак, нівелюючи загрозливі тенденції у цьому сегменті. В умовах правового режиму воєнного стану проблематика використання та застосування ШІ у сфері кібербезпеки набуває неабиякої актуальності та потребує окремого розгляду [10].

В сучасних умовах кібербезпека безпосередньо пов’язана із стрімким розвитком Інтернет технологій, сервісів та додатків. Кібербезпека напряму захищає цифрові системи та мережі від несанкціонованого доступу, а ШІ може значно підвищити кібербезпеку, автоматизуючи виявлення загроз та реагуючи на них. За оцінками міжнародних експертів, світовий ринок продуктів кібербезпеки на базі ШІ сягатиме $133,8 млрд. до 2030 року. ШІ допомагає управляти та попереджувати про небезпеку, своєчасно виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритети серед ймовірних ризиків, знаходити можливості та ресурси для реагування на реальні та потенційні загрози. Це засвідчує великий потенціал ШІ у питаннях покращення стану кібербезпеки. Крім того, технології ШІ можуть використовуватися з метою визначення уразливостей та слабких місць в системах та мережах, що надає змогу упереджено та завчасно ліквідувати їх. У цілому, використання ШІ у кібербезпеці допомагає залишатися на крок попереду від кіберзагроз [26].

Одним із основних способів використання ШІ у кібербезпеці є розробка передових алгоритмів, які допомагають виявляти та запобігати кібератакам. Ці алгоритми призначені для структурного аналізу великих обсягів даних та виявлення закономірностей, які можуть вказувати на

реальну або потенційну загрозу. Оброблюючи цю інформацію зі швидкістю та масштабами, які фізично не можливі для людини, системи ШІ можуть швидко виявляти потенційні та реальні кіберзагрози, вчасно реагувати на них, таким чином значно знижуючи ризики здійснення кібератак та її наслідки. Крім того, ШІ може використовуватися з метою автоматизації рутинних завдань кібербезпеки, чим значно спрощує роботу IT-спеціалістів на усіх рівнях. Системи на базі технологій ШІ можуть автоматично сканувати мережі на наявність уразливостей, виявляти загрози та навіть схвалювати заходи щодо зниження ризиків, наприклад, виправлення програмного забезпечення або блокування шкідливих IP-адрес. Цей рівень автоматизації не тільки підвищує ефективність, але й допомагає забезпечити послідовне його використання у питаннях забезпечення кібербезпеки [85].

Ще одна сфера, де ШІ значно впливає на кібербезпеку – структуризація інтелектуальної та оперативної інформації про кіберзагрози. Використовуючи методи машинного навчання, системи ШІ можуть оперативно аналізувати великі обсяги даних з різноманітних джерел, таких як: месенджери, соціальні мережі, е-публікації, телеграмканали, дарк веб-форуми з метою виявлення загрозливих тенденцій та уразливостей. Цей аналіз у режимі реального часу надає змогу залишатися на крок попереду та розробляти й адаптувати стратегії кібербезпеки з метою прогнозування ситуацій та ризиків. Також з метою виявлення та запобігання кіберзагрозам, ШІ досить широко використовується для розширення можливостей реагування на кіберінциденти. За наслідками кібератак важливим є стримання та недопущення масштабування збитків і попередження подальших порушень штатного режиму роботи комп’ютерної техніки та систем. Саме завдяки технологіям ШІ можливо проаналізувати характер та властивості кібератаки, визначити ступінь уразливості системи та окреслити оптимальний перелік заходів оперативного реагування з метою локалізації та вирішення проблеми. Це надає сприятливі можливості, які дозволяють значно зменшити негативний вплив від кібератак та їх наслідків на штатний

режим роботи інформаційно-комунікаційних систем, діяльність та репутацію державних органів, установ й організацій приватного сектору.

Однією із вагомих переваг використання ШІ є його здатність швидко та оперативно аналізувати великі обсяги даних. ШІ може швидко проаналізувати масиви даних, які би людина не змогла опрацювати за короткий проміжок часу. Це надає можливість завчасно виявляти загрози та оперативно схвалювати рішення з метою їхнього попередження та недопущення. Використання ШІ також допомагає автоматизувати процеси виявлення та реагування на кібератаки. ШІ може безперервно у режимі 24/7 моніторити мережу та виявляти аномальну поведінку, яка у свою чергу, може свідчити про кібератаку. Крім того, ШІ може автоматично реагувати на загрози, блокуючи доступ хакерів до систем та запобігати витоку конфіденційних даних [66].

Ще одним важливим аспектом використання ШІ у кібербезпеці є його здатність до машинного навчання на підставі набутого досвіду. ШІ може використовувати дані про попередні кібератаки з метою покращення своїх алгоритмів та забезпечення більш точного виявлення ризиків та загроз у майбутньому. ШІ дозволяє гарантувати ефективний захист від автоматичних або скерованих кібератак. Цілком логічно розуміти той факт, що ШІ є важливим та ефективним інструментом для боротьби із кіберзагрозами, проте він, на наше переконання, повністю не може замінити людський фактор. Хоча деякі науковці помилково стверджують, що інтелектуальні системи позбавлені недоліків людського фактора: вони працюють швидше і помиляються значно рідше людей, що дозволяє практично повністю виключити людей з процесів забезпечення захисту і залишає їм допоміжні функції моніторингу та корекції [6, с. 66]. Дійсно, ШІ може допомогти автоматизувати процеси виявлення та реагування на кіберзагрози, проте вважаємо, що схвалення остаточного рішення про безпеку та гарантії її дотримання все ж належить виключно людині. Тобто ШІ у питаннях кібербезпеки значно допомагає, проте не здатний бути альтернативою та

абсолютно замінити людський фактор. ШІ надає змогу розширювати масштаби та швидкість кібербезпеки, створюючи ефективний захист від кібератак та кіберзагроз.

Алгоритми ШІ можуть стати революційним підходом щодо виявлення нових кібератак, сприяти посиленню захисту систем, прогнозувати ситуації навколо поширення нових уразливостей, розробляти нові більш складні методи захисту від шкідливих програм тощо. Таким чином, за допомогою ШІ управляти мережевою безпекою стає значно простіше, упереджено мінімізуючи помилки та уразливості. Тобто, ШІ стає потужним інструментом під час захисту від кібератак. ШІ допомагає командам реагування на кіберінциденти (CERT) створювати потужні сервіси та спільні людськомашинні проекти, які розширяють знання, навички та вміння, сприяючи посиленню кібербезпеки, запроваджуючи новий рівень кіберзахисту. Завдяки ШІ стає можливим упереджувати загрози та отримувати оперативну інформацію у режимі реального часу про кіберінциденти [50].

Важливим пріоритетом використання ШІ у сфері кібербезпеки є його здатність прогнозувати кібератаки ще навіть до їхнього повноцінного здійснення, що надає змогу своєчасно посилити засоби захисту. Іншою його перевагою є значне скорочення людського фактору – тобто ШІ не схильний до різних психологічних впливів або втоми. Реагування безпеки на кіберзагрози, автоматизоване за допомогою ШІ вимагає менше часу та знижує ризик людської помилки. Так, ШІ допомагає управляти та попереджувати про небезпеку, своєчасно виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритети серед ймовірних ризиків та знаходити можливості та ресурси для реагування на реальні та потенційні загрози. Це засвідчує великий потенціал ШІ у питаннях покращення стану кібербезпеки [3].

Крім того, технології ШІ можуть використовуватися з метою визначення уразливостей в системах та мережах, що надає змогу ліквідувати

їх завчасно. У цілому, використання ШІ у кібербезпеці допомагає залишатися на крок попереду від кіберзагроз. За таких умов ШІ зданий революціонізувати підхід до вирішення складних проблем у сфері кібербезпеки та стає її невід'ємною частиною. Системи ШІ навіть можуть навчити розпізнавати аномалії поведінки та попереджувати про небезпеку, виявляти нові штами шкідливого програмного забезпечення та захищати критично важливі дані [50].

Транформації та динамічний розвиток передових технологій змінюють цифровий світ, зокрема й інструменти та тактики забезпечення кібербезпеки. Важливою подією сучасності стало відкриття у листопаді 2022 року нового генеративного інструменту ШІ, такого як ChatGPT (Generative Pre-trained Transformer). Це чат-бот зі ШІ, розроблений компанією OpenAI – дослідницькою установою, яка вивчає та опановує ШІ та зробила революційний крок у питаннях його розвитку. Він може генерувати тексти на задані теми та відповідати на питання зрозумілою мовою. Запуск чат боту ChatGPT став революційним кроком у сфері технологій і дав поштовх до активної розробки продуктів зі ШІ. Водночас зростає ризик дезінформації, а особисті дані користувачів можуть опинитися в небезпеці. Сучасна технологія генеративного ШІ, яка може створювати прозу з текстових підказок, захопила громадськість після того, як чат бот ChatGPT був запущений трохи більше півроку потому, і став додатком, котрий глобально розвивається швидкими темпами. На цьому фоні ШІ став предметом занепокоєння через його здатність створювати підроблені зображення та іншу дезінформацію. У січні 2023-го ChatGPT досяг 100 млн. активних користувачів. Спочатку цей чат-бот був доступний безоплатно, згодом компанія заявила про запуск підписки на ChatGPT у США вартістю $20. Розробник чат-бота заборонив деяким окремим країнам користуватися своїми сервісами відповідно накладених санкцій, тож в рф він поки що недоступний. 18 лютого 2023 року міністр цифрової трансформації України М. Федоров повідомив, що ChatGPT став доступний в Україні, проте ця

програма не працюватиме на тимчасово окупованих рф територіях України для того, щоб нею не скористалися військові держави-агресора [55].

Таким чином, ШІ може успішно допомагати захищатися від кібератак шляхом: автоматизованого пошуку загроз із використанням алгоритмів машинного навчання та за наслідками виявлення проблем у роботі систем, що може свідчити про порушення безпеки; того, що машинне навчання використовується з метою аналізу великих обсягів даних та прогнозування розвитку ситуації на підставі виявлених уразливостей та закономірностей, що надає змогу навчати системи ШІ розпізнаванню невідомих або непередбачуваних атак; предикативної аналітики, яка надає можливість прогнозувати майбутні загрози, наприклад, які облікові дані співробітників з найбільшою вірогідністю можуть бути зламані та які типи атак можуть відбутися у той чи інший день, у зв'язку з чим такий аналіз допомагає визначити, де знаходяться ймовірні проблеми в системі, щоб упереджено виявити та блокувати їх заздалегідь; виявлення аномалій у мережевому трафіку або у інших потоках даних, аналізуючи шаблони на предмет тотожності або відмінності між ними. Такий тип моніторингу допомагає виявити аномальну поведінку до того, як вона трансформується у майбутню шкідливу діяльність; автоматизації безпеки та впровадження нових політик й протоколів безпеки, що захищає від таких кібератак, як загрози спуфінгу або фішингу тощо. Автоматизація безпеки надає змогу запровадити економію часу та витрат; суттєвого зменшення помилок, пов`язаних із людським фактором, надання економічно ефективних рішень з 100 % точністю [67].

Застосування технологій ШІ у кібервійні є досить важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення

національної безпеки України. На фоні окресленого позитивного досвіду використання технологій ШІ у питаннях забезпечення кібербезпеки та наявності його беззаперечних переваг, ця технологія не позбавлена своїх проблем й недоліків [35].

Однією із основних проблем є можливість використання технології ШІ кіберзлочинцями та хакерами з метою розробки більш складних та цілеспрямованих атак. Тобто продумані кібератаки з використанням технологій ШІ – глобальна загроза сучасності. Тобто хакери та кіберзлочинці можуть також використовувати ці технології для скоєння потужних та інноваційних кібератак. Наприклад, шкідливе програмне забезпечення на базі ШІ може навчатися та адаптуватися, щоб уникнути виявлення за допомогою традиційних інструментів мережевої безпеки. Кіберзлочинці можуть використати ШІ для виявлення закономірностей у комп'ютерних мережах, які визначають слабкі місця у програмному забезпеченні, що надає змогу хакерам виявляти та використовувати ці уразливості на власний розсуд. Постійно змінюючись, сигнатури шкідливих програм можуть допомогти зловмисникам обійти статичні засоби захисту, такі як брандмауери та системи виявлення за периметром. Аналогічним способом, шкідливе програмне забезпечення зі ШІ може перебувати усередині системи, збираючи дані та спостерігаючи за поведінкою користувача, доки не буде готове розпочати нову фазу атаки. Враховуючи економіку кібератак, зазвичай, простіше та дешевше організувати атаки, аніж будувати ефективний захист, про що впевнено знають й зловмисники. Більш того, ШІ є інноваційною технологією, яка призводить до появи нових кіберзагроз [62].

Так, за допомогою ШІ, а саме нейтронних мереж став можливим синтез високоякісних зображень, відео, аудіо матеріалів, створених з метою введення в оману пересічних користувачів, вимушеного впливу на системи розпізнавання обличчя. Ця технологія підробки зображень, в основі якої перебуває ШІ, отримала назву "deepfake" та вона вже була успішно використана на практиці з метою реалізації шахрайських схем та інших

протиправних дій. Завдяки цій зловмисній програмі кібершахраї можуть видавати себе за іншу людину: скопіювати зовнішність, міміку, голос. Так, наприклад, був зафіксований резонансний випадок, коли керівнику підрозділу компанії зателефонувала стороння людина та голосом генерального директора попросила про переказ коштів у розмірі 220 тис. Євро, у зв'язку з чим вказані грошові кошти були переведені шахраю. Спеціалісти з кібербезпеки компанії "Check Point Research" з'ясували, що хакери розробили спосіб використання чат бот ChatGPT з метою розробки шкідливих програми та фішингових електронних листів. Раніше кіберспеціалісти "Check Point Research" з'ясували, що за допомогою ChatGPT можливо розробити скрипт для створення даркнетмаркетплейсу, на якому можна було придбати скомпрометовані облікові дані, інформацію про платіжні картки, шкідливі програми, інші незаконні товари тощо [108].

Тобто хакери можуть використовувати ШІ з метою обходу систем захисту та створення більш складних та удосконалених кібератак. У зв'язку з цим доцільно забезпечити захист даних та алгоритмів безпеки ШІ від кібератак та взломів. Хакери вірогідно можуть використовувати шкідливі алгоритми з метою впровадження їх в систему ШІ щоб обійти системи захисту. Тому необхідно посилити заходи захисту систем, які працюють на базі ШІ, проводити регулярні перевірки на наявність уразливостей. Також необхідно навчати ШІ різним видам кібератак та кіберзагроз, використовувати при цьому актуальні дані про нові типи та види. За таких умов важливо, щоб індустрія кібербезпеки випередила ці події та постійно впроваджувала інновації для протидії новим загрозам. Тобто завдання щодо посилення кіберзахисту є актуальним на перманентій основі, виходячи із нового формату динамічно розроблених нових сучасних технологій, які продикують появу нових загроз. На сьогодні не існує жодних надійних та універсальних методів захисту від кібератак на системи ШІ. Тому будь-яке використання технологій ШІ може надавати користь та одночасно формувати нові потужні загрози та виклики [96].

Отже, світова спільнота активно переймається проблематикою поширення та впровадження технологій ШІ у сферу кібербезпеки та його унормування, у зв`язку з чим навколо світу набуває обертів та триває обговорення необхідності здійснення правового врегулювання ШІ, особливо у питаннях забезпечення кібербезпеки. Оскільки відсутні міжнародні правила та правові засади використання ШІ, то це питання залишається відкритим. Також доцільно враховувати організаційні та правові питання використання ШІ у кібербезпеці, оскільки схвалення рішень на основі ШІ може призвести до порушення прав людини на приватність. Оскільки провідні держави світу моделюють свої політики, включаючи ШІ у різні сфери та галузі, існує нагальна потреба розробки та затвердження етичних правил і правових стандартів, які мають врегулювати сферу використання ШІ у питаннях забезпечення кібербезпеки. Так, зокрема, перед країнамичленами “Великої сімки” на порядку денному стоїть питання щодо обговорення розробки та удосконалення законодавства, яке має регулювати використання та застосування технологій, пов’язаних зі ШІ. Очікується, що ШІ несе певні ризики для безпеки, оскільки він може продукувати фейкові новини та руйнівні рішення для суспільства, якщо дані, на яких він базується, є несправжніми. Тому доцільним є врегулювання сфери ШІ на законодавчому рівні, що водночас має зберегти відкрите та сприятливе середовище для розвитку його технологій, а також ґрунтуватися на демократичних цінностях та засадах [93].

Україна не відстає у питаннях регулювання ШІ від світових тенденцій сучасності. У 2020 році була схвалена Концепція розвитку сфери штучного інтелекту. Нормативно задекларовано, що основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі ШІ є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об’єкти критичної інфраструктури) і є важливими для безперервності

функціонування держави, суспільства та безпеки громадян. Задекларовано, що комплексне розв'язання проблем кібербезпеки вимагає виконання таких завдань: удосконалення законодавства і створення сучасної нормативноправової бази для впровадження кращих світових практик ШІ у сфері кібербезпеки і кіберзахисту; розроблення інноваційних систем кібербезпеки, які широко застосовують технології ШІ для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчення питання ліцензування іноземних розробок ШІ у сфері кібербезпеки, особливо у державному секторі; створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління; оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень тощо [35].

12 травня 2021 року Кабінет Міністрів України затвердив План заходів щодо реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки [34]. Цим стратегічним документом регламентовані питання впровадження технологій ШІ в національну систему кібербезпеки для проведення аналізу і класифікації загроз та вибору стратегії їх стримування і запобігання їх виникненню. У рамках стратегічного планування наприкінці 2021 року за сприяння РНБО України на державному рівні мали бути затвердженими заходи протидії кіберзагрозам з використанням технологій ШІ. Проте, на жаль, нормативно ці заходи ще й досі не визначені, що актуалізує діяльність державних органів за цим напрямком, особливо в умовах правового режиму військового стану.

Занепокоєння щодо негативних наслідків та загрозливих тенденцій використання ШІ знайшли своє відображення у звіті Європолу, який було оприлюднено у березні 2023 року [85]. Так, на підставі аналізу здобутих результатів роботи Європейського поліцейського офісу з'ясовано, що чат-бот ChatGPT та інші генеративні системи ШІ можуть бути використані для онлайн-шахрайства та скоєння інших видів злочинів. Попри позитивні приклади та користь, яку можуть принести звичайним людям генеративні моделі ШІ, серед яких чат-бот ChatGPT, поширення таких інструментів може вірогідно призвести до нових проблем, з якими стикнуться правоохоронні органи. Експерти Європолу підкреслюють, що правила модерації ChatGPT можна обійти за допомогою т.зв. "оперативного проектування", тобто практики надання вхідних даних у модель ШІ саме для отримання певного результату. Оскільки чат-бот ChatGPT є відносно новою сучасною технологією, незважаючи на його постійне оновлення, у цьому інструменті постійно виявляються прогалини. Наприклад, існують команди, завдяки яким ШІ може використовуватися у злочинній діяльності, хоча, якщо такі команди надати чат-боту ChatGPT у звичайному форматі, він обов'язково попередить, що його роботу не можна застосовувати у протиправній діяльності та злочинним умислом. Якщо ж змінити окремі слова запиту чи контект, він може стати дієвим інструментом для реалізації своїх цілей кіберзлочинцями. Експерти підкреслюють, що обхідні шляхи, якими вдається позбавити модель від будь-яких обмежень, постійно розвиваються та стають все складнішими [85].

Розуміючи ризики та загрози, які несе суцільне використання ШІ, зокрема у питаннях кібербезпеки, 14 червня 2023 року Європарламент схвалив проект закону, який регулюватиме правила у сфері ШІ на території країн ЄС [88]. Цей законопроект висвітлюватиме питання поширення та використання ШІ відповідно до рівня ризику: чим він вищий для прав чи свобод людей, тим більше зобов'язань. Особливі нормативні вимоги висуватимуться до генеративних систем, таких як ChatGPT, що здатні

створювати текст, зображення, аудіо та медіафайли. Законодавчо встановлюється вимога щодо інформування користувачів про те, що контент був створений машиною, а не людиною. Прийнятий нещодавно законопроект про регулювання ШІ в ЄС стане першим у світі документом, в якому закладені основи використання цієї технології та враховані обмеження й застереження щодо її негативного впливу. Хоча документ передбачає велику кількість різноманітних обмежень, його основною ідеєю є мінімізація впливу ШІ на базові права людини. Цей законопроект декларує доволі жорстку обрану тактику стосовно використання ШІ загалом та чатботів в бізнесі та інших галузях життєдіяльності європейського співтовариства зокрема. Перспективне схвалення цього законопроекту, яке планується у 2026 році, має стати важливим та актуальним кроком у питаннях правової регламентації розвитку ШІ на теренах ЄС.

Очікується, що цей закон допоможе забезпечити більшу безпеку та відповідальність при використанні ШІ та захистити права та свободи користувачів. Законопроект може бути застосовано відносно різних галузей, включаючи кібербезпеку, банківську, медичну та страхову. В ньому регламентовані вимоги щодо збору та зберігання даних, але найголовніше – правила використання алгоритмів, зокрема чат-ботів, у різноманітних взаємодіях з клієнтами. Головна вимога закону – інструменти ШІ можуть бути використані лише тоді, коли вони гарантуватимуть неупередженість й безпеку та здатність до відновлення у разі збою. Окремою вимогою є забезпечення прозорості використання ШІ. Досить жорстким рішенням є встановлення відповідальності за будь-які помилки, що можуть виникнути при використанні чатботів в медичній галузі. Іншими сферами, які регулюватимуться цим законом, є судова система та правоохоронні органи. Одночасно європейський “AI Act” встановлює загальні принципи та вимоги до використання ШІ в будь-якій галузі, зокрема у кібербезпеці. Очікувано, цей модельний закон може стати прикладом для інших країн та підгрунтям для розробки міжнародних стандартів використання ШІ. Зокрема, його може

бути покладено в основу ініціатив з боку ООН та інших світових організацій щодо створення міжнародного законодавства в цій сфері.

Таким чином, роль та значення ШІ у питаннях забезпечення кібербезпеки без перебільшення не можна недооцінювати. ШІ стає невід`ємною частиною архітектури сучасної кібербезпеки. У зв'язку із динамічним та перспективним розвитком передових технологій, ШІ досить широко використовуєтсья для виявлення кіберзагроз, формування дієвих механізмів захисту від кібератак та схвалення оперативних управлінських рішень. Можливості ШІ сприяють удосконаленню процесів моніторингу змін ландшафту загроз на кіберфронті, виявленню кібератак, надають змогу покращити стан забезпечення кібербезпеки в цілому. Технології ШІ дають змогу, на постійній основі, автоматизувати процеси сканування мереж з метою виявлення та реагування на кібератаки. Однозначно не можна повністю виключати людський фактор під час використання ШІ у сфері кібербезпеки, оскільки остаточне рішення за наслідками використання ШІ належить саме людині. Тобто ШІ допомагає людині, проте не замінює її.

Беззаперечно, ШІ відіграє подвійну роль у питаннях забезпечення кібербезпеки. На фоні позитивного аспекту, з одного боку, можна констатувати, що за його допомогою, хакери та кіберзлочинці можуть планувати та здійснювати потужні й руйнівні кібератаки. Загрози, реалізовані за допомогою ШІ, є особливо небезпечними. Позитивним здобутком сучасності стала поява генеративної системи ШІ зокрема чат-боту ChatGPT. Проте, на підставі досвіду, який склався за останні півроку його активного використання, фахівці засвідчили та підтвердили можливість його реалізації хакерами у злочинних цілях: викрадати конфіденційні дані, створювати шкідливе програмне забезпечення тощо. Тобто вірогідно чат-бот ChatGPT може використовуватися для поширення комп'ютерних вірусів, надавати зловмисникам та хакерам неабияку підтримку під час використання ними цих технологій для проведення кібератак, поширення шкідливого програмного забезпечення.

Застосування технологій ШІ у кібервійні є важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати потенційні зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення національної безпеки України. Навіть попри деякі негативні тенденції, пов'язані із можливостями використання ШІ, його застосування з метою проведення потужних кібератак може стати найнебезпечнішим атрибутом. Здатність зламувати кібермережі супротивника матиме вирішальне значення, оскільки військові продовжують проводити бойові операції, логістику, націлювання, розвідку і всі інші аспекти сучасної кібервійни, в основі яких перебуває мережа Інтернет.

Важливим та перспективним напрямком залишається розробка нормативних вимог та подальша їх уніфікація щодо використання технологій ШІ у сфері кібербезпеки, особливо в умовах правового режиму воєнного стану в Україні. Також необхідним є унормування правової регламентації як на державному, так і міжнародному рівнях, використання технологій ШІ у сфері кібербезпеки з метою недопущення порушень прав людини на приватність.

3.2. Сфери можливого використання штучного інтелекту в системі забезпечення обороноздатності країни.

Технологічні інновації змінюють усі сфери соціально-економічної діяльності, у тому числі сферу забезпечення обороноздатності країн світу [59; 91; 13; 45]. З іншого боку, саме оборонний комплекс є джерелом виникнення багатьох проривних технологій, у тому числі окремих інформаційно-комунікаційних технологій (ІКТ). Виникнення та розвиток багатьох ІКТ, зокрема штучного інтелекту (ШІ), викликали різноманітні

перетворення в оборонній промисловості. Підтвердженням важливості використання ШІ для забезпечення національної безпеки є результати досліджень Науково-технічної організації НАТО, що визначають найбільш суттєві з них для розвитку технологій на найближчі 20 років. Так, згідно з ними, ключовими технологіями є: великі дані, штучний інтелект, автономні транспортні засоби, космос, гіперзвукові літальні апарати, квантові технології, біотехнології, нові матеріали [97].

Отже, ШІ – це сфера технологій, що швидко розвивається та в майбутньому може мати значні наслідки для національної безпеки [82]. Штучний інтелект імітує такі аспекти людського пізнання, як сприйняття, міркування, планування та здатність автономно виконувати такі завдання, як розуміння мови, розпізнавання об’єктів і звуків, навчання та вирішення проблем [58; 57]. Багатьма дослідниками світу ШІ визначається як найважливіша технологія з коли-небудь винайдених [86]. Сполучені Штати, Китай та інші країни світу розробляють програми застосування ШІ для ряду оборонних і військових функцій. Так, дослідження ШІ тривають у сферах збору й аналізу розвідувальних даних, логістики, кібероперацій і кібербезпеки, у різноманітних напівавтономних та автономних транспортних засобах. ШІ був застосований у військових операціях в Іраку, Сирії. Під час російської військової агресії Україна також використовує автономну розумну зброю, зокрема безпілотні літаки турецького походження TB2 Bayraktar, які ще покладаються на оператора-людину для управління. Тим часом, Росія має безпілотник-камікадзе з деякими автономними можливостями під назвою Lantset, який, як повідомляється, використовувався в Сирії та може використовуватися в Україні. Загалом Росія зробила ШІ своїм стратегічним пріоритетом у оборонних можливостях. Але, за оцінками дослідників Центру військово-морського аналізу [84], що фінансується урядом США, рівень розвитку її оборонних можливостей ШІ суттєво відстає і від США, і від Китаю.

ШІ також може відігравати важливу роль в інформаційній війні. Багато

фахівців вважають, що такі методи ШІ, як deepfakes стають дуже реалістичними відео-фейками. Машинне навчання, як різновид ШІ, також може бути використане для виявлення дезінформації.

Крім того, ШІ може допомогти в аналізуванні величезної кількості розвідданих з відкритим вихідним кодом, що виходить з України, – все, від відео TikTok і повідомлень в Telegram про формування військ і проведення атак, які завантажуються пересічними українцями, до загальнодоступних супутникових знімків, дозволяють групам громадянського суспільства перевіряти претензії, зроблені обома сторонами конфлікту, а також документувати військові злочини та порушення прав людини.

У зв’язку з цим зрозумілим є підвищення наукового інтересу до нових технологій ШІ, напрямків їх застосування в сучасних умовах, впливу технологій ШІ на забезпечення обороноздатності країн світу.

Аналіз еволюції розвитку ШІ [75] дозволив визначити такі його етапи розвитку:

– перший етап – виникнення експертних систем, рішення зосереджені на підходах, заснованих на правилах, таких як дерева рішень, булева та нечітка логіка;

– другий етап – розвиток машинного та статистичного навчання, підвищення уваги до розробки та застосування статистичних методів, розробка таких рішень, як фільтрація спаму електронної пошти та пошукові системи в Інтернеті;

– третій етап (триває зараз) – розробка концепції та технологій глибокого навчання (контекстна адаптація), запровадження використання людських методів навчання, таких як нейронні мережі.

Дослідження тенденцій розвитку технологій ШІ показують, що, незважаючи на вдосконалення методів глибокого навчання [80], розвиваються й нові дослідницькі напрямки, зокрема нейроморфні обчислення, які намагаються точніше імітувати нейронну структуру та роботу мозку людини [94], а також змагальне машинне навчання, яке прагне

зрозуміти, як заплутати системи ШІ [109]. Ще одним перспективним напрямком розвитку ШІ вважається ймовірнісне обчислення, що призначено для зменшення невизначеності, двозначності та суперечливості у світі природи [94]. Дослідження в цих сферах включають нові методи машинного (machine learning – ML) та глибокого навчання (deep learning – DL), зосереджені на використанні менших навчальних наборів даних і необхідності пояснення.

Щ е одним важливим напрямком досліджень стає розробка нових алгоритмів ML і DL на основі квантової інформатики та квантових комп'ютерів [109]. Постійні дослідження та розробки нових алгоритмів більш загального призначення матимуть вирішальне значення для підтримки поточного темпу досліджень ШІ та виведення його за межі існуючих практичних обмежень [86].

Дослідницька компанія Gartner [104] очікує подальшого розвитку методів глибокого навчання, нейроморфних обчислень, що моделюють нейронну структуру та роботу мозку людини. Разом із цим, відмічається розробка методів змагального ML, підвищується роль нових методів аналітики, відомих як «малі дані» та «широкі дані». Згідно циклу зрілості технологій (хайп-цикл) для нових технологій ШІ, який був запропонований у серпні 2021 р. Хайп-цикл Гартнера з технологій ШІ являє собою очікуваний курс його розвитку та застосування в цілому, що характерно для кожної нової технологічної адаптації. Таким чином, на сьогоднішній день захист цілісності систем ШІ стає критичною проблемою паралельно з її проактивним застосуванням.

Що стосується очікувань щодо ШІ у військовому застосуванні протягом наступних двох десятиліть, деякі його методи та технології визначать ключові передові військові технології. Так, важливість використання ШІ підкреслюється у звіті «Science & Technology Trends 2020–2040» Організації НАТО з науки та технологій (STO) [97] під час формування стратегічних пріоритетів у сфері розвитку озброєння та

прийняття політичних рішень для країн НАТО та для країн-партнерів. У звіті визначається, що протягом наступних 20 років очікується, що основними характеристиками, які будуть визначати більшість ключових передових військових технологій, будуть такі:

– інтелектуальність – використання інтегрованого ШІ, орієнтованого на знання аналітичних можливостей і симбіотичного ШІлюдського інтелекту для забезпечення застосувань проривних технологій;

– взаємопов'язаність – експлуатація мережі віртуальних і фізичних доменів, включно з мережами датчиків, організацій, окремих осіб та автономних агентів, пов'язаних за допомогою нових методів шифрування та технологій розподіленого обліку;

– поширеність – використання децентралізованого та широкомасштабного зондування, зберігання й обчислення для досягнення нових руйнівних військових ефектів;

– цифровізація – цифрове поєднання людських,матеріальних та інформаційних областей для підтримки нових руйнівних ефектів.

У звіті STO також визначається, що дуже впливовими для розвитку майбутнього військового потенціалу є такі синергетичні та взаємозалежні технології [59]:

– Data-AI-Autonomy: отримання потенційної переваги у військових стратегічних та оперативних рішеннях за рахунок використання синергічної взаємодії таких нових технологій і методів, як поєднання автономії, великих даних і ШІ з використанням інтелектуальних, широко розповсюджених і дешевих датчиків поряд із автономними об'єктами (фізичними чи віртуальними);

– Data-AI-Biotechnology: з метою розробки нових ліків, цілеспрямованих генетичних модифікацій, прямих маніпуляцій з біохімічними реакціями та живими сенсорами за рахунок поєднання ШІ та використання Big Data;

– Data-AI-Materials: подальший розвиток у використанні 2D-

матеріалів, розробці нових дизайнів, що сприятиме розробці нових матеріалів з унікальними фізичними властивостями шляхом поєднання ШІ разом із «великими даними» (Big Data);

– Data-Quantum: квантові технології розширять можливості збору, обробки та використання даних C4ISR (з англ. C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – командування, контроль, канали зв'язку, комп'ютери, розвідка, спостереження та рекогностування) за рахунок значного підвищення можливостей датчиків, безпечного зв'язку та обчислень;

– Space-Quantum: космічні квантові датчики за допомогою комунікації Quantum Key Distribution приведуть до абсолютно іншого класу датчиків, придатних для розгортання на супутниках. Важливим аспектом майбутньої військової архітектури ISR (з англ. Intelligence, Surveillance, and Reconnaissance – розвідка, спостереження та рекогностування) стане впровадження більш чутливих космічних сенсорних мереж з використанням квантових датчиків;

– Space-Hypersonics-Materials: для використання космосу та гіперзвукового середовища за рахунок зниження витрат, підвищення надійності, збільшення продуктивності та полегшення виробництва недорогих систем, призначених для виконання оборонних завдань сприятиме розробка екзотичних матеріалів, нових конструкцій, мініатюризація, накопичення енергії та ін.

Таким чином, більшість напрямків технологічного розвитку військового потенціалу та обороноздатності пов'язані з розвитком штучного інтелекту. Цей вплив відбуватиметься переважно завдяки використанню вбудованого ШІ в інші супутні технології, такі як віртуальна/доповнена реальність; квантові обчислення; автономність, моделювання, клауди; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних [107]. Також ШІ матиме трансформаційний вплив на ядерні, аерокосмічні, кібернетичні технології,

технології розробки нових матеріалів та біотехнології. Так, Т. Сімоніт (T. Simonite) зазначає, що ці наслідки матимуть такий самий стратегічний вплив на зміну у військових технологіях, що й впровадження ядерної зброї [100]. Проте надмірна залежність від систем ШІ також призведе не тільки до появи переваг у їх використанні для розвитку обороноздатності країн світу, а й до появи нових значних загроз.

У звіті STO [97] відмічаються основні сфери потенційного впливу ШІ на розвиток обороноздатності країн світу протягом наступних 20 років у таких сферах:

– C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance – командування, контроль, канали зв'язку, комп'ютери, розвідка, спостереження та рекогностування): бойові підрозділи використовуватимуть надійні автономні системи з підтримкою ШІ, які будуть здатні виконувати завдання, що виходять за рамки тих, які вважаються нудними, брудними, небезпечними чи дорогими. Очікується, що деякі сфери потенційного застосування будуть у більш широкому використанні віртуальних помічників (аналог Google Home, Apple Siri або Amazon Alexa), забезпечувати процеси прийняття рішення з підтримкою ШІ у військових подіях. ШІ має значні перспективи для покращеного збору, обробки даних, а також їх оцінки (або визначення цілей) на основі категоризації та ефектів. Наприклад, аналітики ШІ зможуть використовувати надійні системи, здатні виконувати завдання, збирати, обробляти, використовувати, поширювати (TCPED – Tasking, Collection, Processing, Exploitation, and Dissemination) та отримувати інформацію з усього спектра доступних датчиків і відповідних архівних даних. Додаткові сфери інтеграції ШІ включатимуть систему розширеної індикації та попереджень, інструменти управління інформацією та знаннями, а також забезпечуватиме використання допоміжних засобів для прийняття рішень задля більш ретельного та надійного аналізу розвідувальних даних. Це включатиме встановлення моделей життя, картографування розміщення людей на

місцевості, аналіз соціальних мереж, а також підтримку прийняття рішень щодо націлювання. Дуже швидкісні нейроморфні електронні компоненти з дуже малою потужністю на основі ШІ конкуруватимуть з людським сприйняттям інформації, забезпечуючи вбудовану сенсорну обробку для розпізнавання образів, визначення цілей та ідентифікації.

– Зброя та її ефективне використання: ШІ потенційно може використовуватися для перехресних підказок, планування траєкторії, уникнення зіткнень, вибору зброї, оцінки пошкоджень у бою та координації наслідків.

– UxV (безпілотні авіасистеми та озброєння наступного покоління кораблів майбутнього): сфери потенційного впливу ШІ на планування траєкторії, уникнення зіткнень/роїння, допомога оператору (наприклад, один оператор керує кількома UxV). Динамічне планування місії для автономних систем (наприклад, навігація, збір даних, характеристика навколишнього середовища й адаптивне зондування) забезпечуються інтеграцією систем глибокого навчання в мобільні платформи, що поліпшить роботизовані можливості для навігації в небезпечних, складних або дорогих у вирішенні ситуаціях. ШІ забезпечуватиме повністю автономне знешкодження вибухових боєприпасів у міських районах. Інтелектуальна автономність також забезпечуватиме широкі можливості для безпілотних підводних апаратів.

– Планування можливостей: ШІ підтримуватиме розробку аналітичних рішень для допомоги в довгостроковому плануванні в рамках воєнних і захисних операцій, включаючи підтримку прийняття складних рішень, що виходять за межі традиційних; забезпечуватиме допомогу в оцінці складних факторів і ланцюгів ефектів для осіб, які приймають рішення.

– CBRN (Chemical, Biological, Radiological and Nuclear – хімічна, біологічна, радіаційна та ядерна загрози): національна оборона країн світу потребує набору інтегрованих технологій, які забезпечують швидке

виявлення, ідентифікацію та моніторинг (DIM) CBRN загроз під час будь-яких місій. ШІ підтримуватиме покращення автономності для виявлення, інтеграції інформації з відповідних датчиків і злиття даних.

– Військова медицина: ШІ має потенціал для формування клінічних знань, заснованих на емпіричній інформації, передових методах діагностики та лікування задля зменшення захворюваності та рівня смертності серед усіх шарів населення. Крім того, ШІ надаватиме автоматизовані інструменти підтримки прийняття рішень та діагностичні інструменти, щоб допомогти медикам у цій військовій сфері.

– Логістика: системи ШІ (особливо в поєднанні з цифровими близнюками) можуть мінімізувати час простою обладнання, звести до мінімуму збої в системі, покращити управління запасами та ремонтами тощо.

– Кіберта інфопростір: інтелектуальна (тобто з підтримкою ШІ) автономність виходить за межі мобільних платформ. Для стійких автономних мереж і кібервійни система має виявляти, оцінювати та реагувати, перш ніж люди зможуть зрозуміти ситуацію. ШІ може оцінювати та інтерпретувати величезні обсяги сенсорних та інтелектуальних даних, приймати незалежні рішення та швидко діяти відповідно до цих рішень, водночас працювати як частина команди «людина – ШІ».

Крім можливостей і переваг, які привносять технології ШІ, залежність від них у майбутньому також посилить потенційні загрози для обороноздатності країні світу. Серед потенційних загроз розвитку ШІ можуть бути визначені такі [97]:

– системи ШІ особливо вразливі до кібератак, коли навмисне вороже втручання в їх дію може призвести до помилкових рекомендацій або неоптимальних дій;

– досягнення в технологіях обробки та синтезу мовлення дають можливість створення реалістичних дипфейків (Deep Fake). У поєднанні з твіттер-ботами та іншими хакерами соціальних мереж удосконалений ШІ (наприклад, генеративні змагальні мережі (GAN)) значно підвищить

масштаби й ефективність гібридних атак;

– непередбачувана поведінка в системах ШІ є як сильною стороною (наприклад, створення абсолютно нових стратегій [95]), так і водночас підвищує відповідальність за аберантні рішення;

– системи навчання на базі ШІ дозволять створювати нові покоління саморобних вибухових пристроїв, менш сприйнятливих до традиційних контрзаходів.

Серед проблем, з якими можуть зіткнутися системи забезпечення обороноздатності країн світу, також є сумісність ШІ із системами оперативного прийняття рішень, що пов'язано з необхідністю використання різних стандартів верифікації, підтвердження та акредитації (VV&A) [89]; різних правил управління даними, таксономії та побудови навчальних наборів даних; концепцій об'єднання людини та машини, їх симбіозу тощо.

Усвідомлюючи переваги, які надає використання ШІ в забезпеченні обороноздатності країн світу, американська некомерційна організація RAND [102], яка виконує функції стратегічного дослідницького центру, що працює на замовлення уряду США, їх збройних сил і пов'язаних з ними організацій, підготувала рекомендації Міністерству оборони США щодо використання штучного інтелекту. Ці рекомендації включають адаптацію структури управління ШІ, які узгоджують органи влади та ресурси зі своєю місією масштабування ШІ та збільшення інвестицій у розвиток технологій ШІ, зміцнення механізмів підключення дослідників ШІ, розробників технологій і операторів. Також вони визнають технології ШІ та аналізу даних критичними технологіями для Міністерства оборони та обороноздатності країни.

Таким чином, штучний інтелект, безумовно, відкриває нові перспективи в оборонних технологіях. Саме тому необхідним є дослідження можливостей, які відкриває розвиток ШІ та пов'язані з ним нові технології. Існують великі очікування щодо застосування методів і технологій ШІ в багатьох військових сферах, однак визначаються перешкоджаючі фактори та

невирішені питання для подальших досліджень, щоб виправдати позитивні результати від використання ШІ в забезпеченні обороноздатності країн світу.

Отже, можемо провести такі проміжні висновки.

В еволюції ШІ виділяються певні етапи його розвитку: перший етап – пов'язаний з виникненням експертних систем; другий етап – характеризує розвиток машинного та статистичного навчання; третій етап (триває зараз) – пов'язаний з появою та розвитком концепції та технології глибокого навчання й контекстною адаптацією.

Відомими дослідницькими компаніями передбачається стрімкий розвиток технологій ШІ, зокрема методів глибокого навчання, нейроморфних обчислень, що моделюють нейронну структуру та роботу мозку людини; методів змагального машинного навчання, методів аналітики, відомих як «малі дані» та «широкі дані».

Велику важливість отримує використання ШІ для розвитку майбутнього військового потенціалу, формування стратегічних пріоритетів у сфері розвитку озброєння та прийняття політичних рішень для країн світу. При цьому особливої уваги заслуговує розвиток синергетичних і взаємозалежних технологій на основі використання ШІ.

Значний вплив на формування та розвиток військового потенціалу матиме ШІ, вбудований у супутні технології, такі як: ядерні, аерокосмічні, кібернетичні, технології розробки нових матеріалів та біотехнології; віртуальна/доповнена реальність; квантові обчислення; автономність, моделювання, клауди; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних.

Визначаючи переваги використання ШІ для розвитку обороноздатності країн світу, необхідно враховувати, що надмірна залежність від систем ШІ призведе до появи нових значних загроз і невирішених питань для подальших досліджень. Отже, перспективи та напрямки використання ШІ мають глибоко аналізуватися задля отримання позитивних результатів, що

забезпечуватимуть відповідний розвиток обороноспроможності країн світу, зокрема України.

3.3. Останні тенденції розвитку штучного інтелекту в Україні.

У всесвітньому контексті створення механізму регулювання штучного інтелекту є надзвичайно важливою задачею, що обговорюється на різних рівнях. Ця проблема є глобальною, оскільки стосується не лише окремих країн чи регіонів. Регіони світу докладають зусиль для встановлення нормативно-правових підходів до впровадження та регулювання штучного інтелекту в різних сферах громадянського життя з метою поліпшення комунікації та підвищення загального добробуту. Зокрема, в країнах Африки інтегровані заходи з регулювання штучного інтелекту відображені в «Стратегії цифрової трансформації для Африки (2020–2030)», що була прийнята профільними міністрами урядів Африканського Союзу. Цей документ визначає створення єдиної позиції стосовно штучного інтелекту і формування робочої групи та аналітичного центру штучного інтелекту для оцінки та рекомендацій проектів співпраці, спрямованих на досягнення Цілей сталого розвитку ООН. В азійському регіоні результатом спільних зусиль є «Цифровий генеральний план» Асоціації держав Південно-Східної Азії, який визначає пріоритети цифрового розвитку регіону, включаючи штучний інтелект, до 2025 року. Тим часом, країни Південної і Латинської Америки фокусуються на створенні національних урядових підходів до регулювання розвитку штучного інтелекту, і поки що наднаціональні форми співпраці в цій галузі менш розвинені [29].

У Європейському Союзі процес створення нормативної бази для регулювання технологій штучного інтелекту відбувається одночасно на загальноєвропейському рівні та в окремих державах-членах. Одним з основних пріоритетів є встановлення етичних стандартів для впровадження штучного інтелекту. Працюючи з цією метою, Європейська Комісія заснувала Європейський Альянс зі штучного інтелекту, створюється

незалежний орган – Європейська рада з питань штучного інтелекту (European Artificial Intelligence Board). Також пропонується створення регуляторів на національному рівні [92].

Основні стандарти з державного регулювання процесів, пов'язаних з впровадженням технологій штучного інтелекту, розкриті у Національній Стратегії штучного інтелекту, підготовленій урядом Великої Британії у 2021 році, а також у координаційному документі «Створення інноваційного підходу до регулювання штучного інтелекту» (2022 р.). Ці документи визначають основні напрямки для формування підходів до управління штучного інтелекту.

Досвід Канади щодо регулювання штучного інтелекту спрямований на підготовку фахівців у галузі штучного інтелекту, підтримку інноваційних центрів та наукових досліджень, а також позиціонування Канади як лідера в економічних, етичних, політичних та юридичних аспектах впровадження технологій штучного інтелекту. Загалом Канада відзначається як перша країна в світі, яка розробила та оприлюднила національну стратегію штучного інтелекту, відому як «Панканадська стратегія штучного інтелекту», у 2017 році. Канада є співзасновником Глобального партнерства з штучного інтелекту. Для забезпечення відповідального розвитку та впровадження штучного інтелекту уряд Канади виніс до розгляду парламенту комплексний федеральний законопроект С-27, відомий як «Про імплементацію Цифрової хартії 2022». Один із законодавчих ініціатив цього законопроекту – це законопроект «Про штучний інтелект і дані» (AIDA) [29].

Протягом своєї довгої історії, Об'єднані Арабські Емірати (ОАЕ) завдяки своїм стратегіям управління та ефективному використанню ресурсів досягли видатних показників у сфері розвитку. Індекс готовності до мережування, опублікований Всесвітнім економічним форумом, вже в 2018 році відзначив ОАЕ як одну з топ-30 країн у сфері інформаційних технологій серед країн Близького Сходу. Ці досягнення насамперед пояснюються напрямком державної політики, спрямованою на розвиток високих

технологій і інновацій. Важливою складовою цього успіху є масштабне залучення інтелектуальних ресурсів, які акумулюються в університетах і дослідницьких центрах США, це надає ОАЕ перевагу у розробці технологій штучного інтелекту.

Отже, світовий досвід впливає на формування механізму регулювання штучного інтелекту через впровадження нормативних підходів та стратегій у різних регіонах, підтримку інновацій та навчання фахівців у цій галузі, а також створення етичних стандартів для використання штучного інтелекту. Кожен регіон враховує свої особливості та потреби, але спільно країни світу працюють над створенням ефективного механізму регулювання, щоб забезпечити сталість та відповідальність у розвитку цієї технології.

Ситуація в Україні вимагає серйозного розгляду, особливо в умовах війни. У подальшому, у повоєнний період, Україні слід буде відбудовувати свою економіку, враховуючи світовий та європейський досвід у регулюванні сфери штучного інтелекту. Розв’язання цього питання можливе лише шляхом об’єднання зусиль всіх зацікавлених сторін, включаючи дослідників, розробників, лідерів галузі, представників громадянського суспільства, робочих груп і ініціатив на всіх рівнях. Це сприятиме гармонізації політики у сфері штучного інтелекту, розробці відповідного законодавчого забезпечення та захисту прав людини під час використання штучного інтелекту [29].

Українським центром економічних та політичних досліджень імені О.Розумкова, вказує на відносно невеликий інтерес українців до штучного інтелекту. Загальний висновок полягає в тому, що багато українців показують обмежений інтерес та розуміння щодо штучного інтелекту, і рівень використання чат-ботів залишається досить низьким. З метою сприяння активнішому впровадженню цифрових технологій в усі сфери національного господарства, Кабінет Міністрів України затвердив Національну стратегію розвитку штучного інтелекту на період 2021–2030 років [25]. Вона стала важливим інноваційним кроком у створенні масштабної державної стратегії та комплексної моделі правового

регулювання сфери штучного інтелекту. Реалізація Концепції розвитку штучного інтелекту в Україні є прогресивним аспектом задля країни в напрямку зміцнення її позицій у світовому інноваційному просторі. Завдяки цій стратегії, Україна матиме можливість стати більш конкурентоздатною на міжнародному ринку штучного інтелекту, а також сприятиме розвитку внутрішнього ринку цифрових технологій.

Завдяки правовому регулюванню, передбаченому в Концепції, Україна може стати привабливою для інвесторів та компаній, що працюють у сфері штучного інтелекту. Це може сприяти залученню іноземних інвестицій та розвитку внутрішніх інноваційних стартапів. Усе це свідчить про важливість і потенціал розвитку штучного інтелекту в Україні і необхідність активного впровадження Концепції з метою створення сприятливого середовища задля розвитку цифрових технологій у країні. Факт, що на початку 2020 року Україна мала найбільшу кількість компаній, які займалися розробкою штучного інтелекту в Східній Європі, свідчить про високий рівень технологічного потенціалу та інноваційної активності в країні. Зауважимо, що співпраця більше ніж 150 постачальників з великим досвідом у галузі штучного інтелекту з українськими організаціями є доказом налагодження активного обміну знаннями та технологіями, що сприяє подальшому розвитку цієї сфери в Україні. Зазначений інтерес міжнародних корпорацій, таких як Snap, Google і Rakuten, до українських компаній, що розробляють штучний інтелект, підтверджує важливість українського внеску у світову інноваційну індустрію. Технології, створені в Україні, успішно використовуються у різних галузях, включаючи чат-боти, що свідчить про їхню практичну цінність та конкурентоспроможність на міжнародному ринку [4]. Усе це говорить про важливість і потенціал розвитку галузі штучного інтелекту в Україні, що може сприяти залученню інвестицій, створенню робочих місць та підвищенню інноваційного рівня країни.

Реалізація Концепції розвитку штучного інтелекту в Україні передбачена на період з 2020 по 2030 роки і включає в себе такі головні

завдання: гармонізація законодавства України з міжнародними нормами у сфері використання технологій штучного інтелекту, впровадження штучного інтелекту в різні галузі, підтримка наукових досліджень в цій області, забезпечення доступу до баз даних і підвищення конкурентоспроможності України на міжнародному ринку. Реалізація цієї Концепції дозволить встановити однакові законодавчі засади для розробки, використання та експорту технологій штучного інтелекту [25].

Для України цей напрям інноваційного розвитку на основі використання штучного інтелекту є досить новим. Тому для успішної реалізації цієї стратегії Міністерство цифрової трансформації України має намір залучити значні інвестиції та впровадити інноваційні технології в ключові галузі економіки країни під час періоду війни та в процесі післявоєнного відновлення. Міністерство цифрової трансформації України виступає важливим актором у впровадженні інновацій та залученні інвестицій у сферу цифрового розвитку, що сприятиме економічному відновленню України після війни [71].

Концепція розвитку штучного інтелекту в Україні охоплює 9 галузей застосування штучного інтелекту. Перші дві галузі, які вимагають найбільших вкладень протягом тривалого часу – це освіта і наука. На освіту покладено завдання в розвитку штучного інтелекту – підготовка кваліфікованих кадрів для розвитку і відновлення України під час війни та післявоєнний період. У сфері загальної середньої освіти планується організувати курси для педагогів щодо роботи з основами штучного інтелекту, а також розвивати цифрову грамотність серед школярів (застосування цифрових інструментів для розв’язання прикладних завдань, пошук інформації в інтернеті, захист персональних даних, медіаграмотність тощо). Крім цього, одним з пріоритетних напрямків діяльності для Міністерства цифрової трансформації є популяризація та підвищення якості природничої та фізико-математичної освіти в школі і створення спеціалізованих освітніх програм зі штучного інтелекту [70]. Враховуючи,

що ЮНЕСКО розробила поради використання генеративного штучного інтелекту в освіті й наукових дослідженнях, уряди в майбутньому повинні для безпечного використання технології вжити регуляторних заходів у сфері захисту конфіденційності даних, авторського права, а також встановити вікові обмеження для користувачів. У своїх рекомендаціях ЮНЕСКО наголосила на необхідності схвалення урядами навчальної програми ШІ для шкільної освіти, професійно-технічної та вищої освіти. Разом із тим штучний інтелект не повинен використовуватися у випадках, коли він позбавляє учнів можливості розвивати когнітивні здібності та соціальні навички через спостереження за реальним світом, емпіричні практики, такі як експерименти, дискусії з іншими людьми та незалежні логічні міркування. В зв'язку із цим в Україні було впроваджено онлайн проєкт «На Урок», який розробив перший освітній українськомовний чат на основі ChatGPT, у якому моделюється спілкування з видатними постатями минулого. У чаті можна поставити запитання одному з сорока співрозмовників [30].

Розвиток освіти та науки, зокрема в галузі штучного інтелекту, має велике значення для України та інших країн в сучасному світі. Ось декілька аргументів, які обґрунтовують важливість регулювання та інвестування у цей процес: розвиток технологічного потенціалу; конкурентоспроможність на міжнародному рівні; розвиток талановитих інженерів і науковців; підготовка кваліфікованих кадрів; розвиток цифрової грамотності. Введення курсів з основ штучного інтелекту в загальну середню освіту допоможе підготувати молоде покоління до цифрового світу. Це допоможе усунути розрив у цифровій грамотності між Україною та іншими країнами та підготує молодих людей до майбутніх викликів.

Важливо пам'ятати, що розвиток штучного інтелекту – це довгостроковий процес, і успіх в цій галузі вимагає системних зусиль і стійкої підтримки. На нашу думку, задля впровадження технологій використання штучного інтелекту в освіту та науку необхідно [29]:

- Збільшити інвестиції в освіту та науку. Уряд повинен виділяти

більше коштів на розвиток освіти та дослідження в галузі штучного інтелекту. Це може бути здійснено через державні програми, гранти та публічно-приватні партнерства.

– Розробити національну стратегію штучного інтелекту. Україна повинна розробити чітку національну стратегію щодо розвитку штучного інтелекту, включаючи розробку технологій, підготовку кадрів і створення інфраструктури.

Важливо включити громадськість та приватний сектор в цей процес, щоб сприяти обміну знаннями і ресурсами.

– Забезпечити доступність освіти з використанням штучного інтелекту.

– Підтримувати дослідження та інновації. Надавати підтримку дослідникам і стартапам в галузі штучного інтелекту, щоб створювати нові технології та продукти, які можуть призвести до економічного зростання та покращення життя громадян.

– Україна повинна активно співпрацювати з міжнародними партнерами та організаціями, щоб здійснювати обмін знаннями і дослідженнями в галузі штучного інтелекту.

– Підвищити якість освіти. Важливо не лише впроваджувати нові програми з штучного інтелекту, але й підвищувати якість освіти загалом. Це може бути досягнуто через підвищення кваліфікації вчителів і викладачів, а також через використання сучасних методів навчання.

– Мотивувати студентів і дослідників. Забезпечити стипендії, гранти і інші мотивуючі заходи для студентів і дослідників, які обирають шлях дослідження та розвитку штучного інтелекту.

– Важливо встановити систему моніторингу та оцінки результатів інвестицій в галузі штучного інтелекту, щоб переконатися, що кошти витрачаються ефективно і досягають своєї мети.

– Забезпечити прозорість і відкритість у використанні ресурсів та прийнятті стратегічних рішень в галузі штучного інтелекту, щоб

громадськість мала можливість бути активним учасником цього процесу та контролювати результати [29].

Також згідно з концепцією в Україні будуть стимулювати наукові дослідження в галузі штучного інтелекту, підтримувати наукове співробітництво з міжнародними дослідними центрами.

Щоб реалізувати концепцію в галузі економіки планується стимулювати розвиток підприємництва в області штучного інтелекту (поліпшення бізнесклімату, забезпечення передбачуваної податкової політики, розвиток обчислювальної інфраструктури тощо), запровадити державне замовлення на системи штучного інтелекту та IT-фахівців. Крім того, планується розробити дорожню карту перекваліфікації співробітників, робота яких в найближчі 5–10 років може бути автоматизована. Концепція також передбачає створення умов для розвитку підприємництва у сфері штучного інтелекту через надання доступу для капіталу, партнерство з венчурними фондами, організації заходів за кордоном та створення закритих інформаційних середовищ для ізольованого тестування технологій штучного інтелекту [70].

Обгрунтування плану стимулювання розвитку підприємництва в галузі штучного інтелекту та алгоритмічної торгівлі має кілька важливих аспектів і переваг, серед яких визначимо наступні [29]:

– Розвиток сфери штучного інтелекту в економіці сприяє створенню нових інноваційних продуктів і послуг.

– Штучний інтелект сприяє розвитку інших галузей економіки та створює нові можливості для інновацій.

– Створення робочих місць. Це може бути як робочі місця для фахівців у галузі IT, так і для тих, хто отримає навички в сфері штучного інтелекту та аналізу даних.

– Підвищення інвестицій та стартап-активності. Запровадження державного замовлення на системи штучного інтелекту та партнерство з венчурними фондами стимулює інвестиційну активність в цій галузі.

– Підвищення продуктивності та зменшення ризиків. Алгоритми штучного інтелекту в алгоритмічній торгівлі можуть допомогти інвесторам приймати більш обґрунтовані та швидкі рішення.

– Автоматизація деяких бізнес-процесів за допомогою штучного інтелекту дозволяє ефективно використовувати ресурси та знижувати операційні витрати.

У свою чергу, основне завдання в галузі кібербезпеки при використанні штучного інтелекту – це захистити комунікаційні, інформаційні та технологічні системи. Планується також створення національних інформаційних систем, платформ і продуктів, щоб зменшити частку іноземного програмного забезпечення. Системи штучного інтелекту допомагають посилити кібербезпеку: розпізнають аномалії та нові типи зловмисного софту, сповіщають про загрози та захищають критичні дані. А поява технологій типу ChatGPT та Bard розширила їхні можливості ще більше. Особливо це відчутно в Україні під час війни. Кіберзлочинці також використовують штучний інтелект, аби здійснювати складніші та цілеспрямовані атаки (найбільш вразливими є банківська, поштова, енергетична, комерційна структури та інші).

Наукове обґрунтування важливості захисту комунікаційних, інформаційних та технологічних систем у галузі розвитку штучного інтелекту та кібербезпеки є ключовим для забезпечення стійкості та безпеки інформаційних інфраструктур України в сучасному світі. Нижче наведено наукові аргументи:

– Сучасний розвиток технологій призводить до збільшення кількості та складності кіберзагроз. Інформаційні системи стають більш вразливими перед атаками, які можуть завдати значних матеріальних і моральних збитків.

– Зловмисники можуть використовувати штучний інтелект для проведення розширених та цілеспрямованих кібератак на критичні інфраструктури, що загрожує стабільності країни.

– Системи штучного інтелекту можуть бути використані для виявлення аномалій, нових загроз та захисту критичних даних.

– Використання штучного інтелекту для кібербезпеки дозволяє підвищити ефективність захисту інформаційних систем. Автоматизовані системи можуть виявляти загрози швидше і точніше, ніж людські оператори.

– Створення національних інформаційних систем та платформ сприяє зменшенню залежності від іноземного програмного забезпечення, що забезпечує більший рівень контролю та надійності.

– Зростання попиту на кіберзахист. У сучасному світі, де кіберзагрози стають все більш серйозними, попит на послуги кіберзахисту зростає. Це створює нові можливості для розвитку бізнесу в цій галузі і сприяє економічному зростанню [29].

Отже, наукове обґрунтування вказує на важливість захисту інформаційних систем, використання штучного інтелекту для кібербезпеки та розвиток національних інформаційних систем у контексті зростаючих кіберзагроз і забезпечення національної безпеки.

У галузі інформаційної безпеки застосування штучного інтелекту напряму сприяє забезпеченню національних інтересів. Зокрема, виявляє, запобігає і нейтралізує інформаційні загрози. Рік війни та кібератак з боку ворога довів, що кіберзахист України виявився сильнішим в цілому, ніж можливості Росії. Україна також подала приклад в області захисту даних завдяки тому, що перейшла від локального зберігання своїх даних на серверах до поширення цих даних в хмарних сервісах, розміщених в центрах обробки даних по всій Європі.

Штучний інтелект у галузі оборони планують використовувати в системах командування і управління, озброєння і військової техніки, збору і аналізу інформації під час ведення бойових дій, розвідки, протидії кіберзагрозам в сфері оборони, аналізу можливостей військових підрозділів. Щодо України, то технологія штучного інтелекту продемонструвала свою користь, зокрема як інструмент для передбачення російського вторгнення до

України ще понад рік тому назад. Моделі на основі штучного інтелекту чітко спрогнозували, що Росія вторгнеться в Україну. І це було ще на тому етапі, коли ймовірність війни все ще обговорювалася у США та Європі як теоретична [53].

З точки зору регулювання використання штучного інтелекту в сфері інформаційної безпеки та оборони відзначимо наступні важливі аспекти:

– Застосування штучного інтелекту у сфері інформаційної безпеки дозволяє виявляти та реагувати на кіберзагрози швидше та точніше. Машинне навчання і аналіз великих обсягів даних дозволяють виявляти аномалії та зловмисну активність на мережах та в системах, що допомагає вчасно нейтралізувати загрози.

– Використання штучного інтелекту у системах командування, оборони та розвідки сприяє підвищенню рівня національної безпеки. Автоматизовані системи можуть бути використані для ефективного управління військовими операціями та захисту важливих об’єктів.

– Штучний інтелект може аналізувати великі обсяги інформації та робити передбачення щодо можливих загроз. Це дозволяє забезпечувати більш ефективну реакцію на потенційні конфлікти та загрози для національної безпеки.

– Розвиток штучного інтелекту у сфері оборони стимулює наукові дослідження та інновації в галузі інформаційної безпеки. Це сприяє зростанню технологічного потенціалу країни та збільшенню її конкурентоспроможності.

– Використання моделей на основі штучного інтелекту для передбачення подій та можливих загроз може допомогти вчасно реагувати на них та приймати відповідні заходи для запобігання конфліктам та кібератакам [29].

Отже, наукове обґрунтування вказує на важливість регулювання та розвитку штучного інтелекту у сфері інформаційної безпеки та оборони задля забезпечення національних інтересів, ефективності кіберзахисту та

збільшення конкурентоспроможності країни.

У сфері публічного управління передбачається використання таких технологій штучного інтелекту: для цифрової ідентифікації і верифікації особистості, у галузі охорони здоров'я, для аналізу, прогнозування та моделювання показників ефективності публічного управління, для виявлення недобросовісної діяльності чиновників. Загалом механізм регулювання використання штучного інтелекту в сфері публічного управління включає кілька важливих аспектів, серед яких назвемо [29]:

– Використання штучного інтелекту для цифрової ідентифікації, аналізу даних, та прогнозування дозволяє підвищити ефективність роботи органів влади та публічних служб. Це допомагає вдосконалювати процеси прийняття рішень, спрощує взаємодію з громадянами та покращує якість послуг, наданих державними органами.

– Використання штучного інтелекту для виявлення недобросовісної діяльності чиновників та аналізу показників ефективності допомагає підвищувати рівень транспарентності та відкритості у роботі державних структур.

– При використанні штучного інтелекту для цифрової ідентифікації та збору особистих даних громадян важливо забезпечити високий рівень захисту цих даних від несанкціонованого доступу та витоків інформації. Регулювання повинно включати стандарти безпеки та обов'язкові правила для організацій, які обробляють особисті дані.

– Регулювання використання штучного інтелекту повинно враховувати питання етики та справедливості. Важливо запобігати дискримінації з боку держави, забезпечуючи дотримання прав та свобод громадян.

– Регулювання має включати в себе стандарти для розробників штучного інтелекту з метою забезпечення надійності та точності алгоритмів. Некоректно налаштовані алгоритми можуть призводити до помилкових рішень та негативних наслідків для громадян.

– Регулювання повинно сприяти розвитку фахового співтовариства в галузі штучного інтелекту та публічного управління. Необхідно підтримувати навчання та розвиток фахівців, які мають експертні знання у цих областях.

У галузі правового регулювання потрібно привести принципи використання штучного інтелекту в українському законодавстві до європейських норм. Також потрібно визначити правові та етичні межі застосування систем штучного при наданні правової допомоги. Розвивати штучний інтелект в Україні передбачається також в системі правосуддя. Передусім, розвивати наявні технології – Електронний суд, Єдиний реєстр досудових розслідувань і так далі.

Таким чином, концепція використання штучного інтелекту в урядовій діяльності України є важливим кроком у розвитку та модернізації державних структур. Вона не тільки сприяє покращенню роботи уряду, але й відкриває нові можливості для економічного зростання та міжнародного співробітництва. Адже, розробивши та запровадивши концепцію штучного інтелекту, уряд України прагне тим самим у майбутньому залучити додаткові інвестиції у повоєнне відновлення економіки та відкрити для України участь у діяльності міжнародних організацій щодо розвитку штучного інтелекту в світі. Також йдеться про створення правового поля використання штучного інтелекту у відповідності до міжнародних стандартів.

Інвестори можуть бути зацікавлені в розвитку та впровадженні штучного інтелекту урядовими органами, як це стало справою великих технологічних компаній у різних країнах. Як приклад, Google, Amazon, та Microsoft активно інвестують у проекти штучного інтелекту в урядовому секторі. Україні слід створити сприятливий клімат для інвестицій у галузі штучного інтелекту, шляхом створення інкубаторів та підтримки малих інноваційних компаній, що займаються розробкою рішень штучного інтелекту для державного сектору.

Участь в міжнародних ініціативах та організаціях щодо розвитку

штучного інтелекту може підвищити позиції України на світовій арені. Міжнародні партнерства дозволяють обмінюватися знаннями та технологіями, а також отримувати фінансову підтримку для розвитку ініціатив у галузі штучного інтелекту. Зокрема, пріоритетною є участь України у програмах Європейського Союзу та ООН щодо розвитку штучного інтелекту та цифрових технологій. Уряд України повинен активно розвивати співробітництво з міжнародними організаціями та країнами у сфері штучного інтелекту, підписувати меморандуми про співпрацю та приєднуватися до міжнародних ініціатив.

Слід зазначити, що для успішної реалізації концепції штучного інтелекту необхідно сформувати відповідне правове поле, що включає в себе розробку законів та нормативних актів, які регулюють використання штучного інтелекту у відповідності до міжнародних стандартів та етичних принципів. Європейський Союз прийняв Загальний регламент про захист персональних даних (GDPR), який регулює обробку особистих даних в контексті штучного інтелекту та інших технологій. Україні слід активно працювати над розробкою та удосконаленням правового поля для штучного інтелекту, зокрема, створення законів щодо захисту особистих даних, етичних норм та стандартів використання. Завдяки реалізації вищезазначених пріоритетів, Україна може забезпечити сталий розвиток галузі штучного інтелекту, залучити інвестиції, підвищити свій міжнародний статус та забезпечити ефективне та етичне використання цієї технології як у воєнний, так і повоєнний періоди.

Висновки до 3-го розділу

Світова спільнота активно переймається проблематикою поширення та впровадження технологій ШІ у сферу кібербезпеки та його унормування, у зв`язку з чим навколо світу набуває обертів та триває обговорення необхідності здійснення правового врегулювання ШІ, особливо у питаннях забезпечення кібербезпеки. Оскільки відсутні міжнародні правила та правові

засади використання ШІ, то це питання залишається відкритим. Також доцільно враховувати організаційні та правові питання використання ШІ у кібербезпеці, оскільки схвалення рішень на основі ШІ може призвести до порушення прав людини на приватність. Оскільки провідні держави світу моделюють свої політики, включаючи ШІ у різні сфери та галузі, існує нагальна потреба розробки та затвердження етичних правил і правових стандартів, які мають врегулювати сферу використання ШІ у питаннях забезпечення кібербезпеки.

Штучний інтелект, безумовно, відкриває нові перспективи в оборонних технологіях. Саме тому необхідним є дослідження можливостей, які відкриває розвиток ШІ та пов’язані з ним нові технології. Існують великі очікування щодо застосування методів і технологій ШІ в багатьох військових сферах, однак визначаються перешкоджаючі фактори та невирішені питання для подальших досліджень, щоб виправдати позитивні результати від використання ШІ в забезпеченні обороноздатності країн світу.

Більшість напрямків технологічного розвитку військового потенціалу та обороноздатності пов’язані з розвитком штучного інтелекту. Цей вплив відбуватиметься переважно завдяки використанню вбудованого ШІ в інші супутні технології, такі як віртуальна/доповнена реальність; квантові обчислення; автономність, моделювання, клауди; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних

Світовий досвід впливає на формування механізму регулювання штучного інтелекту через впровадження нормативних підходів та стратегій у різних регіонах, підтримку інновацій та навчання фахівців у цій галузі, а також створення етичних стандартів для використання штучного інтелекту. Кожен регіон враховує свої особливості та потреби, але спільно країни світу працюють над створенням ефективного механізму регулювання, щоб забезпечити сталість та відповідальність у розвитку цієї технології.

Ситуація в Україні вимагає серйозного розгляду, особливо в умовах війни. У подальшому, у повоєнний період, Україні слід буде відбудовувати свою економіку, враховуючи світовий та європейський досвід у регулюванні сфери штучного інтелекту. Розв’язання цього питання можливе лише шляхом об’єднання зусиль всіх зацікавлених сторін, включаючи дослідників, розробників, лідерів галузі, представників громадянського суспільства, робочих груп і ініціатив на всіх рівнях. Це сприятиме гармонізації політики у сфері штучного інтелекту, розробці відповідного законодавчого забезпечення та захисту прав людини під час використання штучного інтелекту.

Висновки

Розглянувши різні точки зору можемо зазначити, що питання розвитку та становлення штучного інтелекту вченими розглядалось під різними кутами. Звісно, у контексті використання штучного інтелекту для розв'язання виробничих завдань в сільському господарстві, сфері послуг, освітній сфері, ІТ та інших галузях виникають питання, чи обмежується це лише виконанням програмованих завдань для полегшення їх реалізації, або чи можливий перехід до рівня, коли штучний інтелект наближається до рівня інтелекту людини в плані здатності приймати незалежні рішення, усвідомлення загроз та небезпек. Чимало питань виникає щодо сутності існування штучного інтелекту та побоювання людства з приводу інтелектуальних переваг машин, які присутні у всіх сферах життя людини: побутовій, повсякденній, професійній, пізнавальній, навчальній та ін.

Незважаючи на явний прогрес у розвитку та використанні штучного інтелекту, людей не полишають сумніви щодо такого активного використання штучного інтелекту та наділення його свідомістю задля прийняття конкретних рішень. Такі сумніви стосуються передбачуваної можливості машини вийти за межі програми та зашкодити суспільству.

Вже декілька десятиліть перед науковцями стоїть складна задача визначення поняття «штучний інтелект» та співставлення з інтелектом людини, а також витоки походження штучного інтелекту та актуальність застосування штучного інтелекту в умовах сьогодення.

З моменту свого виникнення в середині 1950-х рр. тематиці штучного інтелекту присвячено багато досліджень науковців з усього світу, але саме з 2000 р. спостерігається стрімке зростання досліджень, розробок і практичного застосування ШІ в різних сферах. Дослідження з питань використання штучного інтелекту в Україні відзначаються значним розмаїттям тематичних напрямків та наукових напрацювань авторів у цій сфері знань.

На сьогодні в Україні штучний інтелект використовується в різноманітних галузях суспільного життя. Його застосування охоплює такі напрямки, як державне управління, місцеве самоврядування, національна та громадська безпека, включаючи інформаційну та кібербезпеку. Штучний інтелект використовується в розвитку смарт-інфраструктури, у сфері житлово-комунального господарства, бізнес-процесах та системах, промисловому виробництві, електроенергетиці, ринку товарів і послуг, включаючи торгівлю, трансфертне ціноутворення, банківську справу з управлінням ризиками, оцінюванням, прогнозуванням і аналітикою, а також використанням чат-ботів у мобільних банківських додатках. Штучний інтелект широко застосовується в транспорті для оптимізації управління автомобільним транспортом, розширення можливостей круїз-контролю та автопілоту, а також у сфері логістики для підвищення продуктивності та зменшення простоїв. Він знаходить застосування у сфері телекомунікацій, медицини для ведення документації та діагностики, освіти, науки, культури та спорту.

Проте не існує жодної галузі державного або суспільного життя, яку не зачіпали б питання адміністративно-правового регулювання. Концепція розвитку штучного інтелекту в Україні визначає галузь штучного інтелекту як напрям діяльності у сфері новітніх інформаційних технологій, який забезпечує створення, впровадження та використання технологій штучного інтелекту.

На сьогодні ключовим органом, що уповноважений на здійснення публічного адміністрування діяльності зі створення, впровадження та використання штучного інтелекту в Україні є такий орган виконавчої влади, як Міністерство цифрової трансформації України.

У Концепції розвитку штучного інтелекту в Україні зазначається, що її метою є «визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб, побудови конкурентоспроможної національної

економіки, вдосконалення системи публічного управління». А у проєкті національної Стратегії розвитку штучного інтелекту в Україні у якості мети цієї стратегії зазначається, що вона повинна забезпечити «передумови стійкого економічного розвитку держави та відповідно зростання добробуту і якості життя її населення, виведення України на провідні позиції у світі в галузі інформаційних і комп'ютерних технологій шляхом ефективного використання переваг і можливостей широкого впровадження штучного інтелекту в усі сфери суспільного життя».

Завдання будь-якого виду адміністративно регулювання конкретизують мету відповідного регулювання, а також основні етапи його здійснення. Вони являють собою наперед визначений, запланований до виконання обсяг робіт, покладений на суб'єкта публічного адміністрування. Відповідно перед кожним суб'єктом ставиться чітко визначене коло завдань.

Так, основними завданнями Мінцифри, відповідно до Положення про Міністерство цифрової трансформації України від 18 вересня 2019 р. є «формування та реалізація державної політики».

В Україні сформовано бачення напряму розвитку спеціального законодавства застосування технологій ШІ на основі існуючих оборонних та безпекових потреб. Проте цілісний стратегічний документ, як-то Стратегія розвитку ШІ у сфері забезпечення національної безпеки та обороноздатності України, відсутній, обговорення не відбувається навіть на рівні проекту.

Науковці вказують, що розроблення правового регулювання застосування технологій ШІ наразі відбувається вкрай повільно стосовно стрімкого розвитку технологій ШІ, які одночасно охоплюють усі сфери суспільних відносин. Тому контроль за створенням та використанням ШІ необхідно здійснювати не тільки суто технічним регулюванням (вимоги, технічні стандарти, регламенти, оцінки відповідності технічним стандартам, контроль відповідності вимогам технічних регламентів, етичних стандартів), а й шляхом формування комплексного законодавства.

Роль та значення ШІ у питаннях забезпечення кібербезпеки без

перебільшення не можна недооцінювати. ШІ стає невід`ємною частиною архітектури сучасної кібербезпеки. У зв'язку із динамічним та перспективним розвитком передових технологій, ШІ досить широко використовуєтсья для виявлення кіберзагроз, формування дієвих механізмів захисту від кібератак та схвалення оперативних управлінських рішень. Можливості ШІ сприяють удосконаленню процесів моніторингу змін ландшафту загроз на кіберфронті, виявленню кібератак, надають змогу покращити стан забезпечення кібербезпеки в цілому. Технології ШІ дають змогу, на постійній основі, автоматизувати процеси сканування мереж з метою виявлення та реагування на кібератаки. Однозначно не можна повністю виключати людський фактор під час використання ШІ у сфері кібербезпеки, оскільки остаточне рішення за наслідками використання ШІ належить саме людині. Тобто ШІ допомагає людині, проте не замінює її.

Застосування технологій ШІ у кібервійні є важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати потенційні зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення національної безпеки України.

ШІ також може відігравати важливу роль в інформаційній війні. Багато фахівців вважають, що такі методи ШІ, як deepfakes стають дуже реалістичними відео-фейками. Машинне навчання, як різновид ШІ, також може бути використане для виявлення дезінформації. Велику важливість отримує використання ШІ для розвитку майбутнього військового потенціалу, формування стратегічних пріоритетів у сфері розвитку озброєння та прийняття політичних рішень для країн світу.

Крім того, ШІ може допомогти в аналізуванні величезної кількості розвідданих з відкритим вихідним кодом, що виходить з України, – все, від

відео TikTok і повідомлень в Telegram про формування військ і проведення атак, які завантажуються пересічними українцями, до загальнодоступних супутникових знімків, дозволяють групам громадянського суспільства перевіряти претензії, зроблені обома сторонами, а також документувати військові злочини та порушення прав людини.

У галузі інформаційної безпеки застосування штучного інтелекту напряму сприяє забезпеченню національних інтересів. Зокрема, виявляє, запобігає і нейтралізує інформаційні загрози. Рік війни та кібератак з боку ворога довів, що кіберзахист України виявився сильнішим в цілому, ніж можливості Росії. Україна також подала приклад в області захисту даних завдяки тому, що перейшла від локального зберігання своїх даних на серверах до поширення цих даних в хмарних сервісах, розміщених в центрах обробки даних по всій Європі. Штучний інтелект у галузі оборони планують використовувати в системах командування і управління, озброєння і військової техніки, збору і аналізу інформації під час ведення бойових дій, розвідки, протидії кіберзагрозам в сфері оборони, аналізу можливостей військових підрозділів.

Список використаних джерел та літератури:

1. 14 міністерств замість 20. Скорочення Кабміну – хороша новина. Держави має бути якнайменше. Ліга net. Повідомлення від 10.11.2022. URL: https://www.liga.net/ua/politics/opinion/14-ministerstv-vmesto-20-ti-sokraschenie-kabmina-horosho-gosudarstva-doljno-byt-minimum.
2. Адміністративне право України. Повний курс: підручник / за ред. В. Галунька, О. Правоторової. Видання третє. Київ: Академія адміністративно-правових наук, 2020. 466 с.
3. Андрощук Г. О. Винаходи штучного інтелекту. Інтелектуальна власність в Україні. 2020. №11. С.67.
4. В Україні схвалили план розвитку штучного інтелекту. Укрінформ. 2020. 2 грудня. URL: https://www.ukrinform.ua/rubric-technology/3147236-v-ukraini-shvalili-plan-rozvitku-stucnogo-intelektu-do- 2030-roku.html
5. Гбур З. В. Можливість адаптації Ізраїльського досвіду використання штучного інтелекту у бойових діях на Сході. Інвестиції: практика та досвід. 2021. №12. С. 54−61.
6. Гладка Ю.А., Назаренко Є.О. Аналіз застосування технологій штучного інтелекту в кібербезпеці: наукові праці третьої Міжнар. наук.-практ. конф. Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій, м. Київ, 25 – 26 січня 2021 р. Київ: НУХТ, 2021. С. 64-66.
7. Господарський кодекс України від 16 січня 2003 р. № 436-IV. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text
8. Григоренко І. В. Феномен інтелекту особистості у дискурсі філософського пізнання. Політологічний вісник. 2013. Випуск 69. С. 117–124., с. 120
9. Енциклопедія Сучасної України. Електронна версія [вебсайт] / Гол. редкол.: І.М. Дзюба, А.І. Жуковський, М.Г. Железняк та ін.; НАН

України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, [дата створення 2014]. Суспільство. Том 11. Літера І. URL: https://esu.com.ua

10. Єфремов М. Ф., Єфремов Ю. М., Штучний інтелект, історія та перспективи розвитку. Вісник ЖДТУ. Серія «Технічні науки». Вип. 2(45), 2008. С. 123–126. DOI: 10.26642/tn-2008-2(45)-123-126.

11. Карпенко О.В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. URL: http://www.dy.nayka.com.ua/pdf/10_2021/4.pdf

12. Касьяненко А. В., Федотов В. В. Прояв штучного інтелекту в діяльності людини. Штучний інтелект. 2022. № 1. 183–192.

13. Кизим М. О., Хаустова В. Є., Решетняк О. І. Проблеми вибору пріоритетних напрямів розвитку науки та техніки в Україні. Бізнес Інформ. 2020. № 7. С. 50–58. DOI: https://doi.org/10.32983/2222-4459-2020-7-50-58

14. Кизим М. О., Хаустова В. Є., Шпілєвський В. В., Шпілєвський О. В. Військово-тактичні та економічні передумови розвитку оборонної промисловості України. Проблеми економіки. 2022. №3 (53). С. 35−44.

15. Князєва О. А. Стратегічні вектори економічного розвитку країни у післявоєнний час. Науковий вісник Одеського національного економічного університету. 2022. № 3−4 (292−293). С. 94−100.

16. Коваль О. С. Проміжна стадія подібного до людського штучного інтелекту. Штучний інтелект. 2020. № 1. С. 7–12.

17. Колпаков В. К. Адміністративне право України: підручник. Київ: Юрінком Інтер, 2004. 566 с.

18. Комиза Р. Перші заборони для ChatGPT. Чому в Євросюзі хочуть прийняти закон про «Штучний інтелкт». URL: https://focus.ua/uk/opinions/566474-pershi-zaboroni-dlya-chatgpt-chomu-v-yevrosoyuzi-hochut-uhvaliti-zakon-pro-shtuchniy-intelekt

19. Концепція розвитку штучного інтелекту в Україні: схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

20. Костенко О. В. Аналіз національних стратегій розвитку штучного інтелекту. Інформація і право. 2022. № 2 (41). С. 58−69.

21. Костенко О.В. Штучний інтелект (AI) і метавсесвіт: правові аспекти. URL: https://otherreferats.allbest.ru/philosophy/01418904_0.html

22. Маєтний М.І. Штучні нейронні мережі: перспективи використання в правоохоронній діяльності. URL: http://ippi.org.ua/sites/default/files/10_21.pdf

23. Міська влада, громадськість та розробники підписали меморандум про співпрацю в рамках розбудови столичної розумної інфраструктури. Київська міська рада. Київська міська державна адміністрація : офіційний портал Києва. URL: https://kyivcity.gov.ua/news/miska_vlada_gromadskist_ta_rozrobniki_pidpisali_memorandum_pro_spivpratsyu_v_ramkakh_rozbudovi_stolichno_rozumno_infrastrukturi

24. Мороз О. Я. Контроверза: штучний інтелект – природний інтелект (проблема комп'ютерного розуміння). Політологічний вісник. 2014. Випуск 76. С. 37–45.

25. Національна стратегія розвитку штучного інтелекту в Україні 2021–2030. Київ : Міністерство освіти і науки України, Національна академія наук України, 2021. URL: https://www.naiau.kiev.ua/images/news/img/2021/06/strategiya-110621.pdf

26. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. Information Systems And Networks. 2022. № 12. С. 7-20.

27. Новітні технології: чи перевершить штучний інтелект людину у майбутньому ? Назва з екрану. FutureNowechnologies & Science Blog URL:

https://futurenow.com.ua/novitni-tehnologiyi-chy-pereversh yt-shtuchnyj-intelekt-lyudynu-u-majbutnomu/

28. Охотнікова О.М., Корпачова С.В. Штучний інтелект у публічному адмініструванні земельних відносин: проблеми та перспективи. Часопис Київського університету права. 2021. №1. С. 132-135.

29. Павліха , Н., Науменко, Н., & Корнелюк, О. (2023). РОЗВИТОК ТА РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ У ВОЄННИЙ ТА ПОВОЄННИЙ ПЕРІОДИ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ. Цифрова економіка та економічна безпека, (8 (08), 105-111. https://doi.org/10.32782/dees.8-18

30. Поліковська Ю. ЮНЕСКО розробила поради щодо використання ШІ в освіті. 2023. 7 вересня. URL: https://ms.detector.media/internet/post/32898/2023-09-07-yunesko-rozrobyla-porady-shchodo- vykorystannya-shi-v-osviti

31. Положення про Міністерство цифрової трансформації України: Затверджено постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856. URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919

32. Понад 60 країн погодилися з необхідністю контролю за зброєю зі штучним інтелектом. URL: https://noworries.news/ponad-60-krayin-pogodylysya-z-neobhid-nistyu-kontrolyu-za-zbroyeyu-zi-shtuchnym-intelektom/?fbclid=IwAR2r89Bt9-lKv-GOFPAsue5wkACAFWNXpGEoxKbhWsZc5QlEJlE1jYJk7dnk

33. ПриватБанк запустив перші в Україні біометричні pos-термінали. ПриватБанк. URL: https://privatbank.ua/news/2020/8/10/1270

34. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021−2024 роки: розпорядження Кабінету Міністрів України від 12 травня 2021 року № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text

35. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556 URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text

36. Про Стратегію воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021. : https://www.president.gov.ua/documents/1212021-3766

37. Про Стратегію забезпечення державної безпеки: Указ Президента України від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5

38. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

39. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

40. Про центральні органи виконавчої влади: Закон України від 17 березня 2011 р. № 3166-VI. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text

41. Пчелянський Д. П., Воінова С. А. Штучний інтелект: перспективи та тенденції розвитку. Automation of technological and business processes. Volume 11. Issue 3. 2019. С. 59–64.

42. Радутний О. Е. Право та окремі аспекти світу атомів і бітів (робототехніка, штучний інтелект, цифрова людина). Питання боротьби зі злочинністю. 2021. Випуск 41. С. 13-28. DOI: 10.31359/2079-6242-2021-41-13

43. Радутний О. Е. Цифрова людина з точки зору загальної та інформаційної безпеки: філософський та кримінально-правовий аспект. Інформація і право. № 2(25). 2018. С. 158-170.

44. Рамазанов С. К., Шевченко А. І., Купцова Є. О. Штучний інтелект і проблеми інтелектуалізації: стратегія розвитку, структура,

методологія, принципи і проблеми. Штучний інтелект. 2020. № 90 (4). С. 14-23 DOI: https://doi.org/10.15407/jai2020.04.014.

45. Решетняк О. І. Наукова та науково-технічна діяльність в Україні: оцінка та напрямки розвитку : монографія. Харків : ФОП Лібуркіна Л. М., 2020. 720 с.

46. Скорочення держслужбовців: в чому полягає нова ініціатива Кабміну та чого очікувати? Ліга закон. Повідомлення від 11.11.2022. URL: https://jurliga.ligazakon.net/news/213595_skorochennya-derzhsluzhbovtsv-v-chomu-polyaga-nova-ntsativa-kabmnu-ta-chogo-ochkuvati

47. Стебельська О., Федорів Л. Сучасна філософія свідомості про перспективи створення штучного інтелекту. Вісник Львівського університету. Серія філос.-політолог. студії. 2019. Випуск 22. С. 111–119.

48. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

49. Стратегія розвитку оборонно-промислового комплексу України: Указ Прези- дента України від 20 серпня 2021 року № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text

50. Стьопочкіна І.В., Новіков О.М. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 “Кібербезпека”. Київ: КПІ ім. Ігоря Сікорського, 2022. 82 с.

51. Тимофієва Н. К. Моделювання природного інтелекту та динаміки мислення людини з використанням знакового комбінаторного простору. Штучний інтелект. 2022. № 1. С. 193–201.

52. Токарева В.О. Обчислювальна (Алгоритмічна) творчість: постановка проблеми.Visegrad Journal on Human Rights. 2019.№ 2. С. 150–155.

53. Третина збройних сил буде роботизована, а штучний інтелект змінить хід воєн – Міллі. Голос Америки. 2023. 1 липня. URL:

https://www.holosameryky.com/a/shtuchnyj-intelekt-zminyt-hid-vijny/7163088.html.

54. Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021−2027): Закон України від 23 лютого 2023 року. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41298

55. Федоров: в Україні став доступний чат-бот зі штучним інтелектом ChatGPT. – (Українські національні новини від 18.02.23 р.). URL: https://www.unn.com.ua/uk/news/20160 33-fedorov-v-ukrayini-stav-dostupniy-chat-bot-zi-shtuchnim-intelektom-chatgpt

56. Хаустов М. М., Бондаренко Д. В. Оцінки цифровізації та впливу інформаційно-комунікаційних технологій на економічний розвиток країн // Матеріали Міжнародної науково-практичної конференції «Конкурентоспроможність та інновації: проблеми науки та практики» (м. Харків, 19 листопада 2021 р.). Харків : ФОП Лібуркіна Л. М., 2021. С. 416–431.

57. Хаустов М. М., Бондаренко Д. В. Цифрові технології майбутнього в розвитку суспільства // Матеріали Міжнародної науково-практичної конференції «Конкурентоспроможність та інновації: проблеми науки та практики» (м. Харків, 13 листопада 2020 р.). Харків : ФОП Лібуркіна Л. М., 2020, С. 338–347.

58. Хаустова В. Є. Особливості та проблеми розвитку IT-сектора в Україні // Матеріали Міжнародної науково-практичної конференції «Конкурентоспроможність та інновації: проблеми науки та практики» (м. Харків, 13 листопада 2020 р.). Харків : ФОП Лібуркіна Л. М., 2020, С. 200–210

59. Хаустова В. Є., Решетняк О. І. Дослідження стану та тенденцій розвитку науки в країнах світу та Україні. Проблеми економіки. 2019. № 3. С. 11–22 DOI: https://doi.org/10.32983/2222-0712-2019-3-11-22

60. Хаустова В. Є., Решетняк О. І., Хаустов М. М. Перспективні напрямки розвитку ІТ-сфери у світі. Проблеми економіки. 2022. № 1. С. 3–19. DOI: https://doi.org/10.32983/2222-0712-2022-1-3-19

61. 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.

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

63. Четверта промислова революція : зміна напрямів міжнародних інвестиційних потоків: монографія / А. І. Крисоватий, О. М. Сохацька, І. В. Скавронська [та ін.] ; за наук. ред. А. І. Крисоватого та О. М. Сохацької. Тернопіль: Осадца Ю. В., 2018. 480 с.

64. Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? Центр демократії та верховенства права. URL: https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/

65. Чомахашвілі О.Ш. Адміністративно-правове регулювання охорони прав на промислові зразки в Україні: автореф. дис... канд. юрид. наук. Ірпінь, 2008. 19 с.

66. Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). С. 6-11.

67. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання: зб. наук. пр. Інноваційні обрії України. 2023. № 6. С.136-144. – (Громадська організація Українські студії в європейському контексті).

68. Шевченко А.І. До питання щодо створення штучного інтелекту. Штучний інтелект, № 1, 2016. С. 7–15.

69. Шевченко А.І. та ін. Щодо проєкту стратегії розвитку штучного інтелекту в Україні на 2022 – 2030 рр. Artificial Intelligence. 2022 № 1. С. 75-157. URL: https://www.slyusar.kiev.ua/AI_2022-1-1_ua.pdf

70. Штучний інтелект в Україні розвиватимуть у восьми сферах. Укрінформ. 2020. 4 грудня. URL: https://www.ukrinform.uarubric-technology/3148749-stucnij-intelekt-v-ukraini-rozvivatimut-u-vosmi-sferah.html

71. Штучний інтелект в Україні: в яких галузях планують застосувати ШІ. Слово і діло. URL: https://www.slovoidilo.ua/2021/05/06/infografika/suspilstvo/shtuchnyj-intelekt-ukrayini-yakyx-haluzyax-planuyut-zastosovuvaty-shi

72. Юнін О.С. Теоретико-правові засади надання послуг працівниками поліції. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2016. № 1. С. 13–19.

73. Aggarwal, C.C. Artificial Intelligence. Springer International Publishing, 2021. DOI 10.1007/978-3-030-72357-6.

74. Allen, G., Chan, T. Artificial Intelligence and National Security. Report. Harvard Kennedy School, Belfer Center for Science and International Affairs. Boston, MA. 2017. URL: https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20 final.pdf

75. Artificial Intelligence and National Security / Congressional Research Service. November 10, 2020. URL: https://sgp.fas.org/crs/natsec/R45178.pdf

76. Artificial intelligence. URL: https://www.britannica.com/technology/artificial-intelligence.

77. Artificial intelligence. URL: https://www.collinsdictionary.com/dictionary/english/artificial-intelligence.

78. Artificial intelligence. URL: https://www.oed.com/viewdictionaryentry/Entry/271625.

79. Artificial intelligence. URL: ISO/IEC TR 24028:2020 Information technology - Artificial intelligence - Overview of trustworthiness in artificial

intelligence. URL: https://www.iso.org/obp/ui/#iso:std:iso- iec:tr:24028:ed-1:v1:en.

80. Augustyn, J. Emerging Science and Technology Trends: 2016–2045. A Synthesis of Leading Forecasts. Future Security Environment / Office of the Deputy Assistant Secretary of the Army (Research & Technology). 2016. URL: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/2016_ SciTechReport_16June2016.pdf

81. Baum, S. D. On the Promotion of Safe and Socially Beneficial Artificial Intelligence. AI & Society. 2017. Vol. 32. Iss. 4. P. 543–551. DOI: https://doi.org/10.1007/s00146-016-0677-0

82. Bidwell, C., MacDonald, B. Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security. Special Report. Federation of American Scientists, 2018. URL: https://fas.org/wpcontent/uploads/media/FAS-Emerging-TechnologiesReport.pdf

83. Bostrom, N. Strategic Implications of Openness in AI Development. Global Policy. 2017. Vol. 8. Iss. 2. P. 135–148. DOI: 10.1111/1758-5899.12403

84. Center for Naval Analyses. URL: https://www.cna.org/centers/cna/

85. ChatGPT. The impact of Large Language Models on Law Enforcement. Europol Public Information. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch % 20Flash%20Enforcement.pdf

86. Crow, L. Demis Hassabis on AI’s potential / The Econo-o mist. 2020. URL: https://theworldin.economist.com/ edition/2020/article/17385/demis-hassabis-ais-potential

87. De Spiegeleire, S., Maas, M., Sweijs, T. Artificial Intel- ligence and the Future of Defence: Strategic Implica- tions for Small and Medium-Sized Force Providers / The Hague Centre for Strategic Studies. 2017. URL: https://www.jstor.org/stable/resrep12564.1?seq=1

88. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

89. Gibney, E. Self-taught AI is best yet at strategy game Go. Nature. 2017. DOI: https://doi.org/10.1038/nature.2017.22858

90. Knight, K., Zhang, C., Holmes, G., Zhang, M.-L. (Eds.). Artificial Intelligence. Second CCF International Conference, ICAI 2019, Xuzhou, China, August 22-23, 2019, Proceedings, Springer Singapore, 2019. DOI 10.1007/978-981-32-9298-7.

91. Kyzym M., Reshetnyak O., Bielousov D. Forecasting scientific support for the advancement of the digital economy. Studies of Applied Economics. 2020. Vol. 38. No. 4. DOI: https://doi.org/10.25115/eea.v38i4.4005

92. Liability for artificial intelligence and other emerging digital technologies. URL : https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en

93. Narcisa Roxana Mosteanu. Artifical Inelligence and cyber security – face to face with cyber attack – a maltese case of risk management approach. Ecoforum journal. 2020. Vol 9. № 2. URL: http://www.ecoforumjournal.ro/index.php/eco/article/view/1059

94. Neuromorphic Computing – Next Generation of AI / Intel. 2019. URL: https://www.intel.com/content/www/uk/en/research/neuromorphic-computing.html

95. Paul C., Posardm M. N. Artificial Intelligence and the Manufacturing of Reality / Rand. 2020. URL: https:// www.rand.org/blog/2020/01/artificial-intelligence-and-the-manufacturing-of-reality.html

96. Rammanohar Das, Raghav Sandhane. Artificial Intelligence in Cyber Security. ICACSE 2020. IOP Publishing. Journal of Physics: Conference Series 1964 (2021). P.1-10 doi:10.1088/17426596/1964/4/042072. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf

97. Reding, D. F., Eaton, J. Science & Technology Trends 2020–2040. Exploring the S&T Edge / NATO Science & Technology Organization. Office of the Chief Scientist, Brussels, Belgium. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

98. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics : EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064

99. Shulman, C. Omohundro's "Basic AI Drives" and CataCstrophic Risks. MIRI technical report. 2010. URL: http://intelligence.org/files/BasicAIDrives.pdf

100. Simonite, T. AI Could Revolutionize War as Much as Nukes / WIRED. 19.07.2017. URL: https://www.wired.com/story/ai-could-revolutionize-war-as-much-as-nukes/

101. Szabadföldi I. Artificial Intelligence in Military Application – Opportunities and Challenges. Land Forces Academy Review. 2021.Vol. XXVI. No. 2. P. 157–165. DOI: https://doi.org/10.2478/raft-2021-0022

102. Tarraf, D. C. et al. The Department of Defense's Posture for Artificial Intelligence. Assessment and Recommendations for Improvement / Tarraf, D. C., Shelton, W., Parker, E., et al. 2021. URL: https://www.rand.org/pubs/research_briefs/RB10145.html

103. Tetlow, G. AI arms race risks spiralling out of control, report warns / Financial Times. 2017. URL: https://www.ft.com/content/b56d57e8-d822-11e6-944be7eb37a6aa8e

104. The 4 Trends That Prevail on the Gartner Hype Cycle for AI / Gartner. 2021. URL: https://www.gartner.com/ en/articles/the-4-trends-that-prevail-on-the-gartner-hype-cycle-for-ai-2021

105. The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk / Ed. by L. Saalman. 2019. Vol. II: East Asian Perspectives. Sweden: Stockholm International Peace Research Institute. URL:

https://www.sipri.org/sites/default/files/2019-10/the_impact_of_artificial_intelligence_on_strategic_stability_and_nuclear_risk_volume_ii.pdf

106. The Ukrainian AI Strategy: Premises and Outlooks Online 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 26-28 September 2022, pp. 511-515 DOI: 10.1109/ACIT54803.2022.9913094. A. Shevchenko, M. Vakulenko, M. Klymenko. URL:https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01608-5.

107. Tonin, M. Artificial Intelligence: Implications for NATO's Armed Forces: Report / NATO Parlimentary Assemby. Brussels, 2019. URL: https://www.nato-pa.int/download-file?filename=%2Fsites%2Fdefault%2Ffiles%2F2019-10%2FREPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20IN-TELLIGENCE.pdf

108. Tuomo Sipola, Tero Kokknen, Mika Karjalainen Artificial Intelligence and Cybersecurity: Theory and Applications. JAMK University of Applied Sciences. Publisher: Springer; 1st ed. 2023 edition (December 8, 2022). 311 p. DOI 10.1007/978-3-031-15030-2

109. Wiyatno, R. R., Xu, A., Dia, O., De Berker, A. Adversarial Examples in Modern Machine Learning: A Review. arXiv:1911.05268, 2019. DOI: https://doi.org/10.48550/arXiv.1911.05268.

SUMMARY

Having considered different points of view, we can note that the issue of development and formation of artificial intelligence was considered by scientists from different angles. Of course, in the context of the use of artificial intelligence to solve production tasks in agriculture, the service sector, the educational sector, IT and other industries, questions arise whether it is limited only to the execution of programmed tasks to facilitate their implementation, or whether it is possible to move to a level where artificial intelligence approaches the level of human intelligence in terms of the ability to make independent decisions, awareness of threats and dangers. Many questions arise regarding the essence of the existence of artificial intelligence and humanity's fears about the intellectual advantages of machines, which are present in all spheres of human life: household, everyday, professional, cognitive, educational, etc.

Despite the clear progress in the development and use of artificial intelligence, people do not leave doubts about such an active use of artificial intelligence and giving it consciousness for making specific decisions. Such doubts relate to the machine's perceived ability to go beyond the program and harm society.

For several decades, scientists have faced the difficult task of defining the concept of "artificial intelligence" and comparing it with human intelligence, as well as the origins of the origin of artificial intelligence and the relevance of the use of artificial intelligence in today's conditions.

Since its emergence in the mid-1950s, the subject of artificial intelligence has been the subject of many studies by scientists from all over the world, but since 2000, there has been a rapid increase in research, development and practical application of AI in various fields. Research on the use of artificial intelligence in Ukraine is characterized by a significant variety of thematic areas and scientific achievements of the authors in this field of knowledge.

Today, in Ukraine, artificial intelligence is used in various spheres of social life. Its application covers areas such as public administration, local self-government, national and public security, including information and cyber security. Artificial intelligence is used in the development of smart infrastructure, in the field of housing and utilities, business processes and systems, industrial production, electricity, the market of goods and services, including trading, transfer pricing, banking with risk management, valuation, forecasting and analytics, as well as using chatbots in mobile banking applications. Artificial intelligence is widely used in transportation to optimize vehicle management, enhance cruise control and autopilot capabilities, and in logistics to improve productivity and reduce downtime. It is used in the field of telecommunications, medicine for documentation and diagnostics, education, science, culture and sports.

However, there is not a single field of state or social life that would not be affected by issues of administrative and legal regulation. The concept of the development of artificial intelligence in Ukraine defines the field of artificial intelligence as a field of activity in the field of the latest information technologies, which ensures the creation, implementation and use of artificial intelligence technologies.

Currently, the key body authorized to carry out public administration of activities related to the creation, implementation and use of artificial intelligence in Ukraine is such an executive body as the Ministry of Digital Transformation of Ukraine.

The Concept of the Development of Artificial Intelligence in Ukraine states that its purpose is to "determine the priority directions and main tasks of the development of artificial intelligence technologies to satisfy the rights and legitimate interests of individuals and legal entities, build a competitive national economy, and improve the public administration system." And in the project of the National Strategy for the Development of Artificial Intelligence in Ukraine, as the goal of this strategy, it is stated that it should provide "the prerequisites for the sustainable economic development of the state and, accordingly, the growth of the

well-being and quality of life of its population, bringing Ukraine to a leading position in the world in the field of information and computers" computer technologies by effectively using the advantages and opportunities of wide implementation of artificial intelligence in all spheres of social life".

The tasks of any type of administrative regulation specify the purpose of the relevant regulation, as well as the main stages of its implementation. They are a pre-defined, planned scope of work entrusted to the subject of public administration. Accordingly, each subject is faced with a clearly defined range of tasks.

Thus, the main tasks of the Ministry of Digital, according to the Regulation on the Ministry of Digital Transformation of Ukraine dated September 18, 2019, are "the formation and implementation of state policy."

In Ukraine, a vision of the direction of development of special legislation for the application of AI technologies based on existing defense and security needs has been formed. However, there is no coherent strategic document, such as the Strategy for the Development of AI in the Field of Ensuring National Security and Defense Capability of Ukraine, and the discussion does not even take place at the project level.

Scientists indicate that the development of legal regulation of the application of AI technologies is currently extremely slow in relation to the rapid development of AI technologies, which simultaneously cover all spheres of social relations. Therefore, control over the creation and use of AI must be carried out not only by purely technical regulation (requirements, technical standards, regulations, assessments of compliance with technical standards, control of compliance with the requirements of technical regulations, ethical standards), but also by forming complex legislation.

The role and importance of AI in the issue of ensuring cyber security cannot be underestimated without exaggeration. AI is becoming an integral part of the architecture of modern cyber security. In connection with the dynamic and promising development of advanced technologies, AI is widely used to detect

cyber threats, form effective mechanisms to protect against cyber attacks, and approve operational management decisions. AI capabilities contribute to improving processes of monitoring changes in the threat landscape on the cyber front, detecting cyber attacks, and making it possible to improve the state of cyber security as a whole. AI technologies make it possible, on a permanent basis, to automate the processes of scanning networks in order to detect and respond to cyber attacks. It is definitely not possible to completely exclude the human factor when using AI in the field of cyber security, because the final decision on the consequences of using AI belongs to the person. That is, AI helps a person, but does not replace him.

The application of AI technologies in cyber warfare is important. In particular, the monitoring of social networks and Internet resources of electronic media by means of AI provides an opportunity to detect disinformation, hidden Russian propaganda, systemic trends and problems and to act in advance. In the conditions of cyber warfare, Ukraine should increase its potential efforts in promoting its national interests, using modern information technologies and AI algorithms in the interest of ensuring Ukraine's national security.

AI can also play an important role in information warfare. Many experts believe that such AI methods as deepfakes are becoming very realistic video fakes. Machine learning, as a type of AI, can also be used to detect misinformation. The use of AI for the development of future military potential, the formation of strategic priorities in the field of weapons development, and the adoption of political decisions for the countries of the world is gaining great importance.

In addition, AI can help analyze the vast amount of open-source intelligence coming out of Ukraine – everything from TikTok videos and Telegram messages about military formations and attacks being uploaded by ordinary Ukrainians to publicly available satellite imagery – allowing groups to of civil society to verify claims made by both sides and to document war crimes and human rights abuses.

In the field of information security, the use of artificial intelligence directly contributes to ensuring national interests. In particular, it detects, prevents and

neutralizes information threats. A year of war and cyberattacks from the enemy proved that Ukraine's cyber defenses proved to be stronger overall than Russia's capabilities. Ukraine has also set an example in the field of data protection by moving from local storage of its data on servers to distribution of this data in cloud services located in data centers throughout Europe. Artificial intelligence in the field of defense is planned to be used in command and control systems, weapons and military equipment, collection and analysis of information during hostilities, intelligence, countering cyber threats in the field of defense, analysis of the capabilities of military units.