РОЗДІЛ 5
ТЕОРІЯ ТА ІСТОРІЯ ПОЛІТИЧНОЇ НАУКИ

УДК 327
DOI https://doi.org/10.32782/2663-6170/2023.35.28

«ШТУЧНИЙ ІНТЕЛЕКТ» ЯК ВИКЛИК МІЖНАРОДНІЙ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

ARTIFICIAL INTELLIGENCE AS A CHALLENGE FOR GLOBAL SECURITY SYSTEM

Фурсай О.В.,
аспірант
Навчально-наукового Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

Мета. Метою статті є аналіз зростаючої ролі технології «штучного інтелекту» (ШІ) в сучасних міжнародних відносинах та глобальній системі безпеки, а також визначення сутності впливу цієї технології на зазначені системи.

Результати. Вплив сучасних інформаційних технологій вже давно не обмежується виключно інформаційною сферою, а проникає в політику, економіку, культуру та інші сегменти життя людей. XX та XXI століття стали період, коли темпи технологічного розвитку та глибина проникнення технологій в суспільне життя сягли апогею в своїй історії. Сьогодні світ стикнувся зі ще одним новітнім технологічним інструментом, здатним змінити «правила гри» світової спільноти – технологією «штучного інтелекту».

Як і будь-який новий революційний винахід, який може бути використаний максимально широким колом споживачів інформації, «штучний інтелект» наразі є викликом, особливо безпековим. Потенціал бути використаним для створення кіберзагроз, генерування фейків та поширення дезінформації робить «штучний інтелект», в значні мірі, «терра інкогніта» для держав, бізнесу та громадськості. Враховуючи нерозуміння багатьох аспектів природи та сутності технології, суб'єкти міжнародних відносин стикаються з проблемою формування ефективної системи протидії загрозам, які можуть бути створені з допомогою ШІ.

Тому надзвичайно є актуально є поглиблення вивчення «штучного інтелекту» в контексті його впливу на міжнародну інформаційну безпеку, адже за тільки за умови адекватної оцінки цього впливу можна розбудова надійних інструментів протидії негативним наслідкам використання ШІ.

Наукова новизна. На сьогодні тема використання технології «штучного інтелекту» в контексті аналізу міжнародних відносин, зокрема їх безпекового виміру, є недостатньо дослідженою українськими та закордонними науковцями. Це пов'язано з новизною появи фактору ШІ як однієї з рушійних технологічних сил зміни конфігурації сучасних інформаційних операцій та інформаційної війни.

Практична цінність. Результати статті можуть бути використані науковцями для поглиблення дослідження фактору ШІ в сучасному світовому суспільстві. Також вони можуть бути використані урядовими структурами, зокрема відповідальними за кібербезпеку та захист інфопростору від дезінформаційних кампаній, для адаптації власних систем національної безпеки до нового технологічного виклику, який створив активний розвиток технології «штучного інтелекту».

Ключові слова: «штучний інтелект», інформаційна безпека, технології, інформаційна загрози, кібербезпека, дезінформація, маніпуляція свідомістю, комунікації, медіа, соціальні мережі

The purpose of the article is to analyse the growing role of "artificial intelligence" (AI) technology in modern international relations and the global security system, as well as to determine the essence of the impact of this technology on these systems.

Results. The influence of modern information technologies has not been limited to the information sphere for a long time but permeates politics, economy, culture and other segments of people's lives. The 20th and 21st centuries became the period when the pace of technological development and the depth of penetration of technologies into social life reached their peak in history. Today, the world has encountered another new technological tool capable of changing the "rules of the game" of the world community - the technology of "artificial intelligence". Like any new revolutionary invention that can be used by the widest possible range of information consumers, "artificial intelligence" is currently a challenge, especially a security one. The potential to be used to create cyber threats, generate fakes and spread misinformation does "artificial intelligence" is, to a large extent, "terra incognita" for states, businesses and the public. Given the misunderstanding of many aspects of the nature and essence of technology, subjects of international relations face the problem of forming an effective system for countering threats that can be created with the help of AI. Therefore, it is extremely important to deepen the study of "artificial intelligence" in the context of its impact on international information security, because only under the condition of adequate assessment of this impact, it is possible to develop reliable tools for countering the negative consequences of the use of AI.

Scientific novelty. Today, the topic of the use of "artificial intelligence" technology in the context of the analysis of international relations, in particular their security dimension, is insufficiently researched by Ukrainian and foreign scientists. This is due to the novelty of the appearance of the AI factor as one of the driving technological forces of changing the configuration of modern information operations and information warfare.

Practical value. Scientists can use the results of the article to deepen the study of the AI factor in modern world society. They can also be used by government structures, in particular those responsible for cyber security and the protection of information space from disinformation campaigns, to adapt their own national security systems to the new technological challenge created by the active development of "artificial intelligence" technology.

Key words: "artificial intelligence", information security, technologies, information threats, cyber security, disinformation, mind manipulation, communications, media, social networks

Постановка проблеми. Сучасний етап розвитку міжнародних відносин характеризується високим рівнем впливу технологій, зокрема інформаційних, на політичні, економічні, соціальні та культурні процеси. Однією з таких технологій, яка виникла нещодавно і наразі активно розвивається, є технологія «штучного інтелекту» (ШІ). Варіативність її використання, неочевидні переваги та недоліки ШІ-систем, неготовність світової спільноти оперативно зрозуміти і врегулювати сферу використання ШІ роблять розвиток цієї технології глобальним викликом. Одним із ключових вимірів такого виклику є саме інформаційна безпека, адже інформаційний та кіберпростір є базовими середовищами оперування ШІ.

Аналіз попередніх досліджень та публікацій. Новизна теми ШІ зумовлює наявність хоч і широкої мережі праць, присвячених аналізу сутності та особливостей впливу «штучного інтелекту», але триваючий процес розвитку ШІ, розкриття його багатогранного впливу зумовлюють необхідність в безперервному процесі його осмислення. Для написання цієї роботи були використані як новинні матеріали, так і аналітичні роботи дослідницьких центрів, приватних компаній та державних структур.

Мета дослідження. Проаналізувати роль та вплив технології «штучного інтелекту» (ШІ) на сучасні міжнародні відносини та міжнародну систему інформаційної безпеки.

Методи та прийоми дослідження. Ключовим при дослідженні «штучного інтелекту» як виклику міжнародній інформаційній безпеці стало використання методів аналізу та індукції. Зокрема, методом аналізу було розбито інформаційну безпеку на технічну та «змістовну» складові, та проаналізовано комплексний вплив ШІ на них. Метод індукції був використаний для дослідження різних аспектів впливу ШІ на інформаційну безпеку світу і здійснення висновків щодо того, як «штучний інтелект» впливає на держави, бізнес та громадськість в цілому.

Виклад основного матеріалу. Зростаючий вплив «штучного інтелекту» яскраво демонструє статистика та оцінка суспільством його прогнозованого росту. За прогнозом консалтингової компанії MarketsandMarkets, у 2027 році обсяг світового ринку «штучного інтелекту» сягне 407 млрд доларів, що майже в 5 разів більше, ніж у 2022 році – тоді його обсяг оцінювався у 87 млрд доларів [1]. За підрахунками однієї з найбільших світових інвестиційних компаній Goldman Sachs, використання світовою економікою «штучного інтелекту» може уже в найближчі 10 років спричинити ріст глобального ВВП на 7% або на майже 7 трлн доларів [2].

Також, аналітики міжнародної дослідницької та консалтингової компанії Gartner Inc. прогнозують, що у 2026 році 80% підприємств будуть використовувати у своїй роботі програми або моделі «генеративного штучного інтелекту» – у 2023 році цей показник становив тільки 5% [3].

Таке проникнення ШІ у професійно-виробничі процеси уже спричиняє дискусії у світовому соціумі про майбутню роль людини як працівника. Так, за підрахунками Forbes, проведеного у 2023 році серед понад 2000 працевлаштованих респондентів, 75% опитаних непокояться, що розвиток технології «штучного інтелекту» може спричинити втрату людьми роботи уже протягом 1 року [4]. Ці побоювання не є безпідставними – за словами голови Міжнародного валютного фонду (МВФ) Крісталіни Георгієвої, розвиток ШІ може вплинути на 40% існуючого ринку праці, а в розвинутих економіках це показник може сягати 60% [5].

Вплив стрімкого розвитку ШІ не обмежується виключно економікою як рушійною силою глобального суспільства. Так, ринок ШІ в освіті, який у 2022 році становив 1,2 млрд доларів, уже в 2032 році може зрости до майже 21 млрд доларів [6]. Наразі технологія активно використовується в організації навчальних процесів у школах та університетах, зокрема для пошуку інформації та генерування письмового, аудіо або відео контенту. В політичній сфері ШІ уже зараз активно використовується як інструмент політтехнологій та інформаційних операцій, йдеться, зокрема, про створення діпфейків та генерування неправдивого контенту [7]. На мікрорівні, де оперують виключно споживачі, процеси теж стрімкі – щомісячна кількість користувачів чат-боку ChatGPT уже перевищує 180 млн осіб, а чат-боту Bard від Google – 142 млн користувачів [8].

Як ми бачимо, розвиток технології ШІ уже вийшов за межі дискусії виключно про інформаційно-технологічний поступ людства. Політичний, економічний, соціальний, інформаційний аспекти

впливу «штучного інтелекту» на світ роблять цей феномен фундаментальним фактором розвитку світової спільноти, зокрема системи міжнародних відносин та світової системи безпеки. Так, опитування майже 1500 лідерів у сферах політики, науки, бізнесу, громадськості, опубліковане у звіті The Global Risks. Report 2024 від World Economic Forum (WEF) показало, що світова спільнота відносить потенційні негативні наслідки розвитку технології ШІ в топ-10 глобальних ризиків в довгостроковій перспективі (10 років) [9].

Водночас інформаційна безпека є ключовим виміром глобальної системи безпеки, на який технологія «штучного інтелекту» здійснює найбільш відчутний вплив. У цій статті акцентовано увагу на впливі ШІ на дві складові інформаційної безпеки – технічну, яка традиційно визначається як «кібербезпека», та частина, яка відповідає за захист держав, бізнесу, людей від інформації як носія наративів та меседжів, зокрема від дезінформації.

Якщо говорити про кібербезпеку, то розвиток ШІ створює суттєві ризики використання технології для інформаційних загроз, зокрема кіберзлочинів, деякі з яких уже переросли в загрози. Так, Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) виділяє наступні варіанти використання ШІ для створення кіберзагроз:

– *створення* з допомогою ШІ *фішингових листів*;

– *використання «штучного інтелекту»* хакерами *для удосконалення власного шкідливого програмного забезпечення* (ПЗ). Зокрема, ШІ може «навчити» таке ПЗ уникати систем виявлення, адаптуватися до різних середовищ, визначати і атакувати найбільш вразливі частини системи-цілі. Таке ПЗ в поєднанні з вмонтованим у себе ШІ зможе постійно самовдосконалюватися, навіть за відсутності людського фактору [10].

Одним із найпоширеніших сьогодні методів використання ШІ у зловмисних кіберцілях стало саме створення фішингових електронних листів, ціллю яких є ошукати отримувачів. Зокрема, за допомогою «штучного інтелекту» хакерам вдається створити листи з бездоганною граматикою, точними логотипами та навіть інформацією для входу будь-якою мовою. Процес створення такого листа триває в 10 разів швидше, ніж якби зловмисники створювали їх власноруч [11].

Міжнародна компанія Pirani, яка спеціалізується на ризик-менеджементі для бізнесу, окрім вищезазначених варіантів застосування ШІ, виділяє наступні:

– *соціальна інженерія*, зокрема використання хакерами «штучного інтелекту» для збору та аналізу великих масивів даних про користувачів різних інтернет-платформ;

– *хакерська атака «грубої сили»* (Brute force attack), коли хакери, використовуючи можливості ШІ зможуть ідентифікувати патерни в паролях інтернет-користувачів і генерувати нові [12].

Така варіативність використання «штучного інтелекту» для проведення кібероперацій та наявність спеціалістів, готових експлуатувати «темну» сторону ШІ, створює загрозу виникнення повноцінного ринку надання злочинних послуг з використанням технології. Про це у своєму звіті зазначає одна з найбільших інформаційних-технологічних компаній світу Google. Так, в компанії відзначають, що «в тіні» уже надають такі послуги і ШІ де-факто стає сервісом у світі хакерів [13].

Слід наголосити, що експертиза бізнесу, зокрема таких компаній як Google чи Pirani, є базовою для розуміння викликів для кібербезпеки, які генерує технологія ШІ. Адже саме бізнес є рушійною силою розвитку технології і саме він є її найбільшим користувачем та «жертвою».

Розвиток технології, її можливості для використання хакерами, які постійно збільшуються, зумовлюють погіршення прогнозів щодо кількості кібератак з використанням ШІ. За оцінкою Національного центру кібербезпеки Великої Британії, кількість кібератак та негативні наслідки їх проведення найімовірніше стрімко зростуть в найближчі 2 роки. Зокрема, в центрі наголошують, що уже сьогодні провідні державні та недержавні актори міжнародних відносин, які володіють необхідними ресурсами, експертизою та системою тренування, використовують ШІ у власних кібероперацiях [14].

Підтверджує оцінку британського відомства звіт однієї з найбільших технологічних компаній світу Microsoft, яка також є лідером у розробці технології ШІ. Згідно нього, державні актори уже активно використовують технологію для підтримки власних кібероперацій. Зокрема, хакерська група Forest Blizzard (STRONTIUM), пов'язана з Головним розвідувальним управлінням Міноборони РФ, уже використовує ШІ, зокрема LLM («великі мовні моделі» в наступних цілях:

– *розвідка з допомогою ШІ.* Так, група використовує взаємодію з LLM для кращого розуміння комунікаційних протоколів супутників та специфічних технологічних особливостей самих супутників;

– *підсилене «штучним інтелектом» кодування*. Зокрема, з допомогою ШІ група намагається автоматизувати процес створення шкідливого програмного забезпечення та зробити його не вразливим.

Подібне використання ШІ у зловмисних цілях практикує не тільки Росія – згідно дослідження Microsoft, таку діяльність також зафіксовано щодо хакерських груп Північної Кореї, Ірану та Китаю. Так, наприклад хакерська група Crimson Sandstorm

(CURIUM), афілійована з Іраном, використовує LLM для написання коду, здатного уникати виявлення та виводити з ладу антивірус системи, яка піддається атаці [15].

Таке різноманіття шляхів використання «штучного інтелекту», уже наявні процеси експлуатації ШІ в злочинних цілях як державними, так і недержавними акторами, уже свідчить про поступове трансформування виклику ШІ для світової спільноти в безпосередню загрозу. Цей процес, як показують оцінки державних структур та приватних компаній, буде тільки набирати обертів, що безумовно зробить використанні ШІ в кібероперацiях одним із фундаментальних безпекових трендів найближчих десятиліть.

Окрім викликів в кіберпросторі, інший ризик, який створює ШІ – це загроза збільшення масштабів дезінформації та покращення її якості. Так, опитування World Economic Forum, показало, що уже зараз суспільство вважає згенеровану ШІ дезінформацію 2-им найголовнішим глобальним ризиком сьогодення. Поступається вона тільки глобальним погодним катаклізмам, які традиційно турбують світову громадськість, особливо в умовах сучасних змін клімату [16].

Аналітики WEF в дослідженні Global Cybersecurity Outlook 2024 виділяють 6 сфер, де «штучний інтелект» може бути використаний для негативного впливу на соціально-політичні процеси в державах, зокрема тих, де проводиться виборчий процес:

− безпосередньо *дезінформація,* зокрема використання контенту, згенерованого ШІ, для розповсюдження неправдивої інформації в соцмережах та медіа, а також для маніпулювання свідомістю;

− *створення аудіо та відео діпфейків,* які з удосконаленням технології ШІ буде все важче відрізнити від справжніх відео та аудіо;

− *автоматизована дезінформація*, зокрема використання алгоритмів ШІ для автоматизованого та швидкого поширення дезінформації каналами комунікації, зокрема у великих обсягах;

− *таргетована реклама*, зокрема використання ШІ мікротаргетингу шляхом наданням користувачам соцмереж персоналізованої реклами, ціллю якої є маніпуляція їх поглядами;

− *захист персональних даних.* Йдеться про використання ШІ для обробки великої кількості персональних даних людей;

− *маніпуляція алгоритмами соцмереж.* Використання соцмережами у своїй роботі алгоритмів, де ключовим є використання ШІ, створює загрозу потенційного маніпулювання роботою ШІ задля створення конкретних політичних меседжів [17].

Використання ШІ в таких цілях уже фіксується з боку Росії, Китаю, Північної Кореї та Ірану. Так, компанія Microsoft зафіксувала, що хакерська група Charcoal Typhoon (CHROMIUM), афілійована з владою Китаю, використовує ШІ для перекладу та генерування контенту, який спрямований на маніпулювання свідомістю споживачів інформації [15].

На прикладі України та держав колективного Заходу, яка зазнає гібридної агресії Росії, уже можна спостерігати також кейси використання Кремлем «штучного інтелекту» для здійснення вищезазначених дій. Так, прикладом використання фейку, згенерованого ШІ, стало поширення в соцмережах фейкових аудіо та відео, де екс-Головнокомандувач Збройних Сил України Валерій Залужний нібито закликає військових захопити владу в Україні та критикує Президента України Володимира Зеленського. Ці відео та аудіо були створені на основі діпфейків, згенерованих «штучним інтелектом» [18, 19].

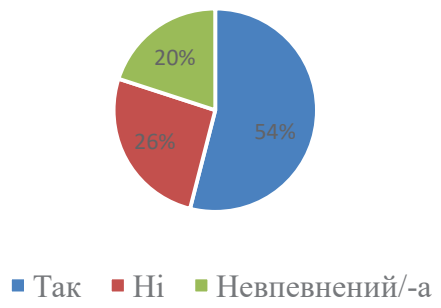
Окрім цього, в березні 2022 року, на початку повномасштабного вторгнення РФ в Україну, російські ботоферми активно поширювали звернення Володимира Зеленського, де він нібито заявляє про «капітуляцію України» та закликає українську армію «скласти зброю». Для створення цього відео також була використана технологія діпфейку. Його творці сподівалися таким чином дестабілізувати ситуацію в Україні, посіяти хаос і, як наслідок, зламати обороноздатність держави [20].

Проблема використання ШІ для генерування таких діпфейків стала настільки поширеною у світі, що можливостей громадського фактчекінгу уже недостатньо для ефективного і оперативного спростування. Тому окремі держави, зокрема Франція, ініціюють створення інструментів виявлення діпфейків. Так, запущений у Францією проєкт DeTOX, який фінансується французьким урядом, концентруватиметься на виявленні діпфейків відомих цивільних та військових персоналій Франції. Для цього розробники використовуватимуть технологію ШІ [21].

Описана вище проблема використання «штучного інтелекту» дезінформації уже гостро сприймається світовою громадськістю. Згідно вищезгаданого опитування Forbes Advisor, 76% опитаних стурбованою проблемою дезінформації, яка може бути згенерована «штучним інтелектом», зокрема такими сервісами як ChatGPT, Google Bard чи Bing Chat. З них тільки половина вважає, що може відрізнити, який контент згенерований «штучним інтелектом», а який – людиною (див. Графік 1).

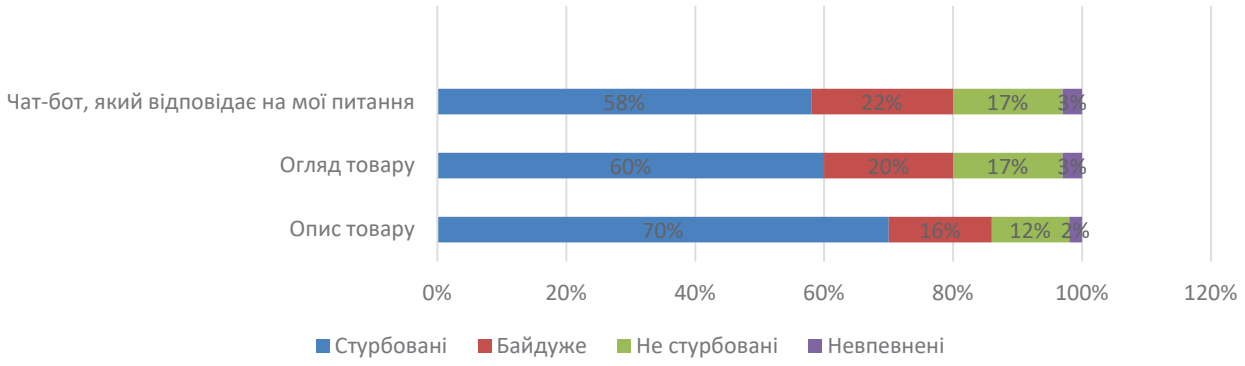
Окрім цього, люди побоюються використання бізнесом технології «штучного інтелекту» для введення в оману покупців. Так, 70% опитаних стурбовані використані ШІ при формуванні опису продукту (див. Графік 2) [22].

Все це зумовлює необхідність регуляторного реагування держав, яке б передбачало встановлення чітких меж використання ШІ та формувало механізми



Графік 1: Чи можете ви відрізнити, де контент згенеровано ШІ, а де людиною?

Джерело: опитування Forbes Advisor (2023)



Графік 2: Типи контенту, використання ШІ щодо яких викликає найбільші хвилювання споживачів

Джерело: опитування Forbes Advisor (2023)

міжнародного співробітництва у цьому питанні. Проте, як і в більшості випадків реагування на появу сучасних технологій, державне чи міжнародне регулювання суттєво відстає від темпі науково-технологічного поступу. Так, на сьогодні переважна більшість держав та міжнародних організацій не мають чіткої регуляторної рамки щодо ШІ, а їх позиції обмежуються виключно деклараціями.

Головною з них в контексті міжнародної кооперації наразі є Декларація Блетчлі з безпеки використання ШІ, підписана в листопаді 2023 року 28 державами та Європейським Союзом. Вона, зокрема, встановлює безпечне, людиноцентричне та відповідальне використання ШІ як базовий принцип розвитку і використання технології. Для цього держави взаємодіятимуть як між собою, так і з бізнесом, науковим середовищем, громадськістю. Щодо самого процесу розвитку технології, то у цьому питанні держави наголосили на важливості прозорості та інклюзивності цього процесу [23].

Що ж до безпосередньо суб'єктів міжнародних відносин, то тут ми можемо спостерігати уже певні ознаки формування регуляторної рамки щодо ШІ. Так, в жовтні 2023 року Президент США Джо Байден видав наказ щодо безпечного, захищеного і надійного використання ШІ, який, зокрема, передбачає:

– вимогу до розробників найпотужніших ШІ-систем ділитися з урядом результатами власних тестів безпеки та іншою критичною інформацією;

– необхідність розробки стандартів розвитку та використання ШІ, зокрема це стосується стандартизування тестування таких систем;

– захист від ризиків використання «штучного інтелекту» для розробки небезпечних біологічних матеріалів;

– захист американців від зловмисних дій, базованих на використанні ШІ;

– започаткування розвинутої програми кібер-захисту, яка б передбачала використання ШІ для виявлення вразливостей в критично важливому програмному забезпеченні.

Загалом, наказ сконцентрований на важливості захисту персональних даних американців як базової умови розвитку технології «штучного інтелекту». Водночас слід зауважити, що цей наказ не є повноцінною регуляторною рамкою використання ШІ і Білий Дім уже працює з Конгресом над створенням закону, який би регулювання питанні ШІ [24].

У процесі формування нормативно-правової бази також перебуває Європейський Союз. Зокрема, наразі Європарламент розглядає запропонований Єврокомісією «Акт про «штучний інтелект» (AI Act), який встановлює чіткі рамки використання ШІ у різних сферах життя європейського суспільства. Наразі це найбільш комплексний та багатогранний документ, який регулює розвиток та використання технології, адже він деталізує саме поняття «штучного інтелекту», чітко встановлює сфери, де його використання заборонено, а також передбачає цілеспрямовану інноваційну політику ЄС щодо перетворення Європи у світового лідера розвитку ШІ [25, 26].

Синхронізовано з Євросоюзом свою регуляторну рамку поступово розробляє й Україна. Так, в жовтні 2023 року Міністерство цифрової трансформації представило дорожню карту з регулювання «штучного інтелекту» в Україні, у фокусі якої – захист прав українців в умовах зростаючого проникнення ШІ в сучасний інформаційний простір. За словами Віце-прем'єр-міністра з інновацій, розвитку освіти, науки та технологій – Міністра цифрової трансформації Михайла Федорова, особливо важливим є використання ШІ у сфері військових технологій.

В дорожній карті наголошується, що в основі впровадження регулювання ШІ лежить bottom-up підхід. Він передбачає спочатку отримання бізнесом інструментів для підготовки до майбутніх вимог, а уже тоді ухвалення профільного закону. Таким чином, влада прагне надати час бізнесу для підготовки до появи регулювання сфери ШІ [27].

Висновки. Розвиток технології «штучного інтелекту» ставить комплексний виклик для всього світу. Ту швидкість та глибину, з якою ШІ проникає у всі сфери життя суспільства, можна порівняти хіба що з проникненням інтернету. Суспільства не встигають за розвитком технології як в частині усвідомлення усіх ризиків, загроз, переваг та недоліків ШІ, так і в частині реагування. Такий вакуум знань та дій дозволяє авторитарним державам, зокрема Росії, Китаю, КНДР та Ірану використовувати ШІ з ціллю впливу на колективний Захід. Це найчастіше проявляється у використанні ШІ на двох напрямах:

- підтримка кібероперацій;
- створення та поширення дезінформації.

Ці безпекові ризики, а зачасту і загрози, уже змушують державних та недержавних акторів адаптовувати свою діяльність відповідно до сучасних викликів. Це, зокрема, проявляється в початку процесу формування регуляторної бази, яка б встановила чіткі рамки використання технології. Цей процес відбувається як на національному, так і на наднаціональному рівнях. Слід зазначити, що цей процес відбувається достатньо повільно і не встигає за реаліями сьогодення.

Особливо це актуально для України, яка стикається з використання ШІ Росією як у інформаційній площині через створення фейків, так і у інструментах ведення бойових дій. Прискорення розвитку наступальних і оборонних інструментів ШІ, а також чітке законодавче регулювання цією сфери – це не просто вимога часу для України, але й питання стратегічної обороноздатності держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Artificial Intelligence. MarketsandMarkets URL: https://www.marketsandmarkets.com/mega_trends/artificial_intelligence#
2. Generative AI could raise global GDP by 7%. Goldman Sachs. – 2023. URL: https://www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html
3. Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026. Gartner Inc.. – 2023. URL: https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026
4. Haan K. Over 75% Of Consumers Are Concerned About Misinformation From Artificial Intelligence. Forbes Advisor. – 2023 URL: https://www.forbes.com/advisor/business/artificial-intelligence-consumer-sentiment
5. Georgieva K. AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity. IMF Blog. – 2024. URL: https://www.imf.org/en/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity
6. Global Generative AI in Business Market. Markets.us. – 2023. URL: https://market.us/report/generative-ai-in-business-market
7. Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics. Insikt Group. – 2023. URL: https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf
8. Demand Sage. Demand Sage URL: https://www.demandsage.com
9. The Global Risks. Report 2024. World Economic Forum. – 2024. – №19. – С. 8
10. Ntalampiras S. ARTIFICIAL INTELLIGENCE AND CYBERSECURITY RESEARCH. G. Misuraca, P. Rossel., 2023. – 39 с.

11. Palma B. AI is transforming cybersecurity: How can security experts respond? World Economic Forum. – 2024. URL: https://www.weforum.org/agenda/2024/01/arms-race-cybersecurity-ai/

12. Jiménez M. Artificial intelligence to combat cyber attacks. Pirani. – 2024. – URL: https://www.piranirisk.com/blog/artificial-intelligence-to-combat-cyber-attacks

13. Cybersecurity Forecast 2024. Insights for future planning. – 2023. URL: https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf

14. The near-term impact of AI on the cyber threat. National Cyber Security Centre. – 2024. URL: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

15. Staying ahead of threat actors in the age of AI. Mocrosoft. – 2024. URL: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai

16. The Global Risks. Report 2024. World Economic Forum. 2024. №19. С. 7

17. Global Cybersecurity Outlook 2024 Geneva: World Economic Forum, 2024. – 39 с.

18. ВІДЕОФЕЙК: Валерій Залужний записав звернення, де наказує військовим покинути зону бойових дій та захоплювати владу. VoxCheck. – 2023. – URL: https://voxukraine.org/videofejk-valerij-zaluzhnyj-zapysav-zvernennya-de-nakazuye-vijskovym-pokynuty-zonu-bojovyh-dij-ta-zahoplyuvaty-vladu

19. ВІДЕОФЕЙК: Валерій Залужний створив петицію про мобілізацію депутатів Верховної Ради. VoxCheck. – 2023. URL: https://voxukraine.org/videofejk-valerij-zaluzhnyj-stvoryv-petytsiyu-pro-mobilizatsiyu-deputativ-verhovnoyi-rady

20. Deepfake video of Volodymyr Zelensky surrendering surfaces on social media The Telegraph. – 2022. URL: https://www.youtube.com/watch?v=X17yrEV5sl4

21. DeTOX: A french-funded project on deepfake detection targeting important civilian and military personalities in France. EURECOM. – 2023. URL: https://eurecom-blog.medium.com/detox-a-french-funded-project-on-deepfake-detection-targeting-important-civilian-and-military-23c30262ee3d

22. Haan K. Over 75% Of Consumers Are Concerned About Misinformation From Artificial Intelligence. Forbes Advisor. – 2023. URL: https://www.forbes.com/advisor/business/artificial-intelligence-consumer-sentiment/

23. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. GOV.UK. – 2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

24. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. The White House. – 2023. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence

25. Fernhout F. The EU Artificial Intelligence Act: our 16 key takeaways. Stibbe. – 2024. URL: https://www.stibbe.com/publications-and-insights/the-eu-artificial-intelligence-act-our-16-key-takeaways

26. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. EUR-Lex. – 2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

27. Регулювання штучного інтелекту в Україні: Мінцифри презентувало дорожню карту. Урядовий портал. – 2023. URL: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuvalo-dorozhniu-kartu