**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Карпатський національний університет імені Василя Стефаника

Факультет історії, політології і міжнародних відносин

Кафедра міжнародних відносин

**ДИПЛОМНА РОБОТА**

**на здобуття другого ( магістерського) рівня вищої освіти**

**на тему: «ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ) НА ГЛОБАЛЬНИЙ МІЖНАРОДНИЙ РОЗВИТОК: БЕЗПЕКОВИЙ АСПЕКТ»**

**Виконала:** студентка
ІІ року навчання ОР Магістр
групи МВ-2м
**спеціальності:** 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Максимюк Неля Миколаївна

**Науковий керівник:**
кандидат політичних наук,
старщий викладач кафедри міжнародних відносин
Голуб'як Н.Р.
**Рецензент:**
кандидат історичних наук,
доцент кафедри міжнародних відносин
Гаврилишин П.М.

Допущено до захисту

«____» _____ 2025 р.

Івано-Франківськ, 2025

**ЗМІСТ**

# ВСТУП

Проблематика впливу штучного інтелекту (ШІ) на глобальний міжнародний розвиток набуває все більшої актуальності в умовах стрімкого технологічного прогресу. Використання ШІ в різних сферах суспільної діяльності, зокрема у безпековому контексті, відкриває нові можливості для підвищення ефективності державного управління, військової справи, економічного розвитку та інформаційної безпеки. Однак, водночас виникають серйозні ризики, пов’язані з неконтрольованим використанням технологій штучного інтелекту, що можуть мати значний вплив на міжнародну стабільність та безпеку.

Сучасний міжнародний розвиток характеризується взаємопов’язаністю глобальних процесів, де технологічні інновації відіграють ключову роль. Штучний інтелект став одним із головних рушіїв трансформаційних змін у різних сферах, включаючи безпеку, оборону, економіку та соціальні відносини. Використання алгоритмів машинного навчання, нейронних мереж та автоматизованих систем прийняття рішень дозволяє значно підвищити ефективність аналізу даних, прогнозування загроз та управління складними ситуаціями. Водночас стрімке поширення таких технологій супроводжується численними викликами, зокрема загрозами кібербезпеці, можливістю створення автономних систем зброї та етичними дилемами, пов’язаними з відповідальністю за прийняття рішень.

У контексті безпекового аспекту впливу ШІ особливої уваги заслуговує питання кібербезпеки. Сучасні цифрові технології стали невід’ємною частиною життєдіяльності держав та організацій, проте їх використання супроводжується ризиками кібератак, витоку конфіденційної інформації та зловживання можливостями штучного інтелекту. З одного боку, ШІ сприяє розробці ефективних механізмів кіберзахисту, включаючи системи виявлення аномалій та аналізу загроз у реальному часі. З іншого боку, зловмисне використання ШІ може стати потужним інструментом для проведення

кібератак нового рівня, що створює додаткові загрози для міжнародної стабільності.

Ще одним важливим аспектом є використання штучного інтелекту у військовій сфері. Розвиток автономних бойових систем, здатних діяти без безпосереднього контролю людини, викликає серйозні дискусії щодо їхньої відповідності міжнародним нормам гуманітарного права та можливих наслідків для світової безпеки. Такі системи можуть значно підвищити точність та ефективність військових операцій, проте водночас існує ризик неконтрольованих дій або технічних збоїв, що можуть призвести до непередбачуваних наслідків.

Етичні аспекти застосування штучного інтелекту у сфері безпеки також є предметом активних дискусій. Виникають питання щодо відповідальності за рішення, ухвалені алгоритмами, потенційної дискримінації або упередженості в процесі автоматизованого аналізу даних, а також можливості маніпулювання інформацією та створення дезінформаційних кампаній. У зв’язку з цим міжнародне співтовариство стикається з необхідністю розробки ефективних механізмів регулювання та контролю за впровадженням ШІ, щоб уникнути можливих негативних наслідків.

**Актуальність дослідження** визначається необхідністю забезпечення балансу між розвитком інноваційних технологій та мінімізацією пов’язаних з ними ризиків. Вивчення впливу ШІ на безпеку в міжнародному контексті дозволяє оцінити потенційні загрози, розробити ефективні стратегії їхнього попередження та сприяти формуванню міжнародної політики, орієнтованої на безпечне використання штучного інтелекту.

**Метою дослідження** є аналіз впливу штучного інтелекту на глобальну безпеку, визначення основних викликів та ризиків, а також розробка рекомендацій щодо мінімізації загроз і забезпечення ефективного міжнародного контролю за розвитком ШІ.

Для досягнення цієї мети у роботі поставлено такі **завдання**:

- дослідити концепцію штучного інтелекту, його принципи функціонування та можливості;

- розглянути роль ШІ у трансформації міжнародного середовища;

- визначити безпекові аспекти впливу ШІ у глобальному контексті;

- проаналізувати основні загрози кібербезпеці, пов’язані із застосуванням ШІ;

- оцінити ризики використання автономних бойових систем;

- розглянути етичні дилеми впровадження ШІ у сфері безпеки;

- дослідити міжнародні механізми регулювання розвитку ШІ;

- визначити роль міжнародної співпраці у забезпеченні безпечного використання ШІ;

- запропонувати стратегії мінімізації ризиків у технічному, політичному та соціальному аспектах.

**Об’єктом дослідження** є процес впливу штучного інтелекту на міжнародну безпеку.

**Предметом дослідження** є безпекові аспекти застосування штучного інтелекту у глобальному міжнародному середовищі.

**Методи дослідження.** У даній роботі використовувалися загальнонаукові та спеціальні методи дослідження:

- аналіз наукової літератури та синтез для вивчення теоретичних положень, систематизації та узагальнення інформації про вплив ШІ на міжнародну безпеку.

- методи системного підходу для дослідження ШІ як багатоаспектної системи в контексті глобального міжнародного розвитку.

- порівняльний аналіз для зіставлення регулятивних підходів різних міжнародних акторів до ШІ-технологій та їх безпекових стратегій.

- SWOT-аналіз для ідентифікації сильних і слабких сторін, а також можливостей та загроз, пов’язаних із впровадженням ШІ.

- методи кількісного і якісного аналізу для всебічної оцінки сучасного стану безпекових загроз та їхнього потенційного впливу на міжнародні відносини.

**Інформаційна база дослідження** ґрунтується на працях таких вчених як А. Труба, О. Кемінь, О. Корнута, П. Норвіг, які присвятили свої роботи питанням штучного інтелекту, міжнародної безпеки та глобального розвитку. Інформаційною базою також є міжнародні нормативно-правові акти, доповіді міжнародних організацій, аналітичні матеріали з питань кібербезпеки та штучного інтелекту, а також результати експертних досліджень у цій сфері.

**Новизна роботи** полягає у комплексному аналізі безпекових аспектів штучного інтелекту, а також у розробці практичних рекомендацій щодо зниження ризиків, пов’язаних із його використанням у міжнародному контексті.

**Практичне значення дослідження.** Магістерська робота має практичне значення у тому, що її основні положення та висновки можуть бути використані для державних установ при розробці національних стратегій кібербезпеки та політики у сфері використання критичних ШІ-технологій. Результати дослідження також можуть слугувати теоретико-методологічною основою для подальших наукових розробок, а також бути включені до навчального процесу вищих закладів освіти в курсах із міжнародної безпеки.

**Структура роботи** включає вступ, три розділи, висновки та список використаних джерел.

# РОЗДІЛ І
# ТЕОРЕТИЧНІ ОСНОВИ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА БЕЗПЕКУ В МІЖНАРОДНОМУ КОНТЕКСТІ

## 1.1. Концепція штучного інтелекту: сутність, принципи функціонування та можливості

Сучасний розвиток технологій значно посприяв популяризації штучного інтелекту (ШІ), що, у свою чергу, спричинило зростання його попиту в різних сферах діяльності. Головною метою застосування ШІ є підвищення ефективності людської діяльності, оптимізація витрат ресурсів, а також автоматизація рутинних процесів. Однією з ключових можливостей ШІ є обробка великих обсягів даних, що дозволяє швидко отримувати аналітичні висновки, скорочуючи затрати часу та зусиль людини.

З точки зору сутності, штучний інтелект можна визначити як систему, що здатна збирати, аналізувати та зберігати інформацію, а також робити висновки на основі отриманих даних відповідно до поставлених завдань. Проте на сучасному етапі розвитку технологій автономний аналіз джерел інформації та самостійна постановка завдань поки що не є обов'язковими характеристиками ШІ. В табл. 1.1 наведено узагальнені визначення ШІ.

Таблиця 1.1

**Визначення штучного інтелекту**

| Визначення штучного інтелекту |
|---|
| Штучний інтелект (ШІ) – це здатність інженерних систем обробляти, використовувати та вдосконалювати отримані знання й навички. |
| ШІ передбачає здатність машин імітувати людський розум і когнітивні здібності, а також адаптуватися до зовнішніх умов, аналізуючи дані та приймаючи рішення на їх основі. |
| Це можливість машин і програм аналізувати інформацію, формувати висновки, постійно навчатися та ефективно застосовувати накопичені знання. |
| Системи зі штучним інтелектом можуть виконувати інтелектуальні процеси, притаманні людям, зокрема міркувати, інтерпретувати інформацію, узагальнювати та враховувати досвід минулого. |

*Джерело: розроблено автором на основі [1-4]*

Штучний інтелект (ШІ) став однією з найважливіших технологій сучасності, яка має потенціал змінити всі сфери людської діяльності. Його розвиток охоплює кілька етапів – від перших програм, що моделювали людське мислення, до сучасних алгоритмів глибокого навчання та великих мовних моделей. Однак шлях становлення ШІ був непростим – технологія пережила періоди піднесення та спаду, коли очікування не завжди відповідали реальним можливостям. В табл.1.2. представлено етапи розвитку штучного інтелекту.

Таблиця 1.2

**Етапи розвитку штучного інтелекту**

| Період | Подія | Опис |
|---|---|---|
| Народження ШІ (1952–1956) | Створення першої програми ШІ | 1955 – Аллен Ньюелл і Герберт Саймон розробили **Logic Theorist**, яка змогла довести 38 із 52 математичних теорем та запропонувала нові докази для деяких з них. |
| | Виникнення терміну «штучний інтелект» | 1956 – Американський інформатик **Джон Маккарті** на конференції в Дартмуті вперше вжив термін «штучний інтелект». |
| Золоті роки ШІ (1956–1974) | Поява першого чат-бота | 1966 – **Джозеф Вайценбаум** створив **ELIZA**, яка імітувала розмову з психотерапевтом. |
| | Розробка першого робота | 1972 – В Японії з'явився перший інтелектуальний людиноподібний робот **WABOT-1**. |
| Перша «зима штучного інтелекту» (1974–1980) | Зупинка фінансування | Через технічні труднощі та завищені очікування **наукові дослідження ШІ втратили фінансову підтримку**. |
| Бум AI (1980–1987) | Розвиток ШІ як наукової дисципліни | 1980 – **Перша національна конференція Американської асоціації штучного інтелекту** в Стенфордському університеті. |
| Друга «зима AI» (1987–1993) | Втрата інтересу до ШІ | Висока вартість та невідповідність очікувань змусили інвесторів **припинити фінансування** досліджень. |
| Поява інтелектуальних агентів (1993–2011) | Перемога над чемпіоном світу з шахів | 1997 – Комп'ютер **IBM Deep Blue** переміг **Гаррі Каспарова** в шаховому матчі. |
| | Вихід AI у побут | 2002 – **З'явився Roomba**, перший робот-пилосос. |
| | Використання ШІ в бізнесі | 2006 – Компанії **Facebook, Twitter та Netflix** почали застосовувати алгоритми ШІ для аналізу даних. |
| Deep Learning, Big Data та штучний загальний інтелект (2011–дотепер) | Розвиток Watson | 2011 – **IBM Watson** переміг у вікторині **Jeopardy!**, довівши здатність розуміти природну мову. |
| | Інтеграція ШІ у мобільні сервіси | 2012 – Google представив **Google Now** – систему персоналізованих рекомендацій. |
| | Використання ШІ в медицині | 2020 – **Baidu створив алгоритм LinearFold AI**, що передбачав послідовність РНК вірусу SARS-CoV-2 |

| | | |
|---|---|---|
| | | за 27 секунд (у 120 разів швидше за інші методи). |

*Джерело: розроблено автором на основі [5]*

Отже, як ми бачимо з табл.1.2, розвиток штучного інтелекту демонструє циклічність – періоди активного розвитку змінюються «зимами», коли через технічні та фінансові обмеження дослідження втрачають підтримку. Однак сучасні досягнення у сфері глибокого навчання, аналізу великих даних та автоматизації відкривають перед людством нові можливості. Від першої програми до інтелектуальних асистентів – штучний інтелект вже сьогодні формує майбутнє технологій, і його потенціал лише зростає.

Штучний інтелект відіграє дедалі важливішу роль у сфері міжнародних відносин, де аналіз великих обсягів даних є ключовим для ухвалення стратегічних рішень на глобальному рівні. У дипломатії, геополітиці та міжнародній економіці обробка інформації та прогнозування сценаріїв розвитку ситуації вимагають високоточного аналізу, який часто виходить за межі людських можливостей. Алгоритми машинного навчання дозволяють штучному інтелекту швидко аналізувати дані з відкритих джерел, виявляти тренди та прогнозувати можливі сценарії розвитку міжнародних подій, що значно підвищує ефективність дипломатичних та політичних стратегій.

Значні інвестиції в розробку ШІ сприяли його інтеграції у різні сфери міжнародної діяльності, включно з економічною дипломатією, торговельними переговорами та аналізом ризиків глобальних фінансових ринків. Штучний інтелект використовується не лише як аналітичний інструмент, а й як фактор економічного впливу, що визначає конкурентоспроможність держав та міжнародних організацій. У сфері інформаційної політики та стратегічних комунікацій ШІ застосовується для аналізу громадської думки, розробки дипломатичних повідомлень і навіть прогнозування впливу міжнародних санкцій або економічних криз. Крім того, популяризація штучного інтелекту як інноваційної технології сприяє зростанню інвестиційної привабливості країн, що лідирують у його розробці.

У фінансовій сфері ШІ широко застосовується для оцінки кредитних ризиків, моніторингу глобальних фінансових потоків та виявлення незаконних транзакцій, що особливо важливо для боротьби з фінансуванням тероризму та відмиванням коштів. Водночас сучасні моделі використання штучного інтелекту часто орієнтовані на короткострокову вигоду, тоді як його довгострокове застосування у сфері міжнародних відносин потребує більшої адаптивності та стратегічного підходу. На нашу думку, у майбутньому ефективність ШІ значною мірою залежатиме від міжнародних норм і стандартів його використання, зокрема у питаннях етики, безпеки та державного регулювання.

Таким чином, штучний інтелект є багатофункціональним інструментом, що сприяє підвищенню ефективності у різних сферах діяльності, проте його стратегічне застосування потребує подальшого дослідження та вдосконалення.

Системи штучного інтелекту працюють, поєднуючи великі обсяги даних з інтелектуальними ітеративними алгоритмами обробки. Це дозволяє їм навчатися на основі шаблонів і особливостей аналізованих даних. Щоразу, коли система виконує цикл обробки інформації, вона тестує та вимірює свою продуктивність, використовуючи результати для подальшого вдосконалення.

Розглянемо детальніше основні компоненти штучного інтелекту.

Так, ШІ не існує без таких ключових елементів [5]:

- машинне навчання (Machine Learning, ML) – дає ШІ можливість навчатися за допомогою алгоритмів, які виявляють закономірності та генерують інсайти на основі аналізованої інформації;

- глибоке навчання (Deep Learning) – підкатегорія ML, яка дозволяє ШІ імітувати нейронну мережу людського мозку. Завдяки цьому система здатна розпізнавати закономірності, шуми та джерела плутанини в даних;

- нейронні мережі – основа глибокого навчання, що імітує нейрони або клітини мозку. Вони складаються з трьох шарів: вхідного, прихованого та

вихідного, містять тисячі або мільйони вузлів, які змінюють ваги зв’язків для оптимізації результатів навчання.

Залежно від рівня автономності та навчання, ШІ поділяється на чотири категорії, які представлені на рис.1.1:


Рисунок 1.1 – Категорії штучного інтелекту

*Джерело: [5]*

Розглянемо детальніше кожну з категорій, що представлені на рис.1.1:

- чисто реактивні системи – не мають пам’яті, працюють у межах однієї конкретної сфери. Наприклад, шахові алгоритми, які обирають найкращий хід у реальному часі;

- системи з обмеженою пам’яттю – накопичують попередні дані та використовують їх для прийняття рішень. Наприклад, рекомендаційні системи, що пропонують ресторани на основі місцезнаходження користувача;

- теорія розуму – передбачає здатність ШІ розуміти думки та емоції, що дозволяє йому соціально взаємодіяти;

- самосвідомі машини – гіпотетичний майбутній рівень ШІ, що володітиме самосвідомістю та інтелектом, подібним до людського.

Штучний інтелект також поділяється за призначенням і технологіями навчання. Вибір відповідного ШІ значною мірою залежить від аналізу методів, за якими він навчався та буде продовжувати своє навчання. Правильний підбір технології навчання відіграє важливу роль, адже використання невідповідного методу може призвести до некоректних результатів у певній сфері діяльності. Залежно від технології навчання штучний інтелект поділяється на чотири основні типи, що відрізняються за принципами розпізнавання інформації, аналізу закономірностей, прогнозування та реакції на отримані дані.

Перший тип – це ШІ, що використовують машинне навчання. Це найпоширеніший варіант, який базується на внесенні інформації у систему за допомогою математичних моделей або алгоритмів. Після аналізу даних штучний інтелект виявляє закономірності та формує прогнози.

Точність таких прогнозів залежить від обсягу та якості вхідних даних. Внесення нової або виключної інформації може спричинити помилкові висновки, оскільки ШІ не враховує змістовне значення груп даних, їх походження чи людські виняткові ситуації. Для отримання якісних прогнозів потрібна ретельна підготовка даних, що вимагає значних зусиль фахівців.

Основна перевага цього підходу – можливість оцінити якість моделі та даних перед побудовою прогнозів. Однак, складність налаштування такого ШІ робить його вузькоспеціалізованим, що унеможливлює його використання для інших завдань без суттєвих змін у моделі. Наприклад, система, розроблена для виявлення шахрайства у банківському секторі, не може бути застосована у виробничому процесі без значних модифікацій.

Другий тип – це ШІ для обробки природної мови. Такий штучний інтелект аналізує текст, розбиваючи його на токени, проводить синтаксичний і семантичний аналіз, а також генерує відповіді на основі попередніх запитів або пошуку аналогій у базах даних.

Він не підходить для економічного аналізу чи створення математичних прогнозів, але може використовуватися як допоміжний інструмент для збору

інформації або взаємодії з користувачем. Головним недоліком є врахування всіх джерел без винятку, що може призвести до прирівнювання малокомпетентних думок до професійних висновків.

Третій тип – це системи комп'ютерного зору, що аналізують зображення та відео. Вони ідентифікують об'єкти на основі їхніх характеристик і конвертують отримані дані у відповідний формат. Цей тип ШІ є доповнюючим і використовується, наприклад, у маркетингу для аналізу поведінки споживачів. Проте його застосування у стратегічному плануванні є обмеженим.

Четвертий тип – це ШІ з глибоким навчанням. Він базується на використанні нейронних мереж і поступово покращує точність результатів з часом. Цей метод мінімізує необхідність участі людини у підготовці даних, перетворюючи трудовитрати спеціалістів у час роботи ШІ.

Однак через це знижується якість прогнозів, оскільки система може включати сумнівні джерела інформації та не враховувати людську непередбачуваність.

Наприклад, система IBM WATSON, яка аналізувала медичні дані, рекомендувала лікування, що могло погіршити стан пацієнтів. У сфері економіки використання такого ШІ обмежене через складність перевірки якості вхідних даних. Він може ефективно працювати лише в умовах повністю автоматизованого середовища без впливу людського фактора.

Сучасні розробки спрямовані на створення ШІ, що відповідатиме "теорії розуму", тобто зможе розпізнавати емоції, наміри та когнітивні процеси людини. Це дозволить покращити аналіз дипломатичних відносин, прогнозувати поведінку міжнародних акторів і сприяти прийняттю ефективних рішень у сфері зовнішньої політики. Однак на даний момент жоден ШІ не здатний самостійно формувати комплексну стратегію міжнародної взаємодії. Лише системи на основі машинного навчання можуть використовуватися як інструменти для аналізу великих масивів

геополітичних даних, що допомагає дипломатам, аналітикам та політикам ухвалювати стратегічні рішення.

## 1.2. Роль штучного інтелекту у трансформації міжнародного середовища

Перед тим як аналізувати сучасний вплив штучного інтелекту (ШІ) на міжнародне середовище, варто розглянути більш детально його історичний розвиток, який ми захопили на початку дослідження. На нашу думку, усвідомлення еволюції цієї технології від перших концепцій до сучасних можливостей дає змогу краще зрозуміти, як і чому ШІ став ключовим фактором глобальної трансформації. Різні науковці по-різному визначають початок розвитку штучного інтелекту, спираючись на історичні та культурні традиції.

Ще в давнину людство формувало уявлення про автоматизовані системи. У давньогрецькій міфології існував образ Талоса – механічного захисника Криту, а в китайських легендах згадується Чжуге Лянь, який нібито створював дерев'яних автоматонів [6]. Це свідчить про те, що ідея штучного інтелекту (ШІ) була закладена в культуру задовго до її практичної реалізації.

Офіційний початок сучасної історії ШІ припадає на середину XX століття. У 1943 році Воррен Маккаллох і Волтер Піттс запропонували математичну модель нейронних мереж [7], а в 1950-му Алан Тюрінг розробив концепцію тесту Тюрінга для оцінки здатності машини імітувати людський інтелект [8]. У 1956 році на конференції в Дартмуті було введено термін «штучний інтелект» [9], що стало відправною точкою для досліджень у цій сфері.

Розвиток ШІ відбувався хвилеподібно: періоди активного прогресу змінювалися етапами стагнації. У 1960-х роках були створені перші

експертні системи, проте в 1970–1980-х ентузіазм згас через недостатні результати та високу вартість досліджень. Новий етап почався у 1990-х із розвитком машинного навчання, а у 2010-х відбувся прорив завдяки глибокому навчанню, зокрема технологіям AlphaGo і GPT [10].

Ще в 1983 році Д. Нейсбіт у своїй книзі «Мегатренди», використовуючи контент-аналіз, зазначав, що тренди як коні: на них легше їхати туди, куди вони прямують [11]. Він визначив десять основних мегатрендів того часу, і першим назвав перехід від індустріального суспільства до інформаційного, прогнозуючи майбутнє за комп'ютеризацією та інформатизацією.

Друга половина XX століття ознаменувалася технічними проривами в інформаційній сфері. Наприклад, у 1953 році інженер М. Купер, батьки якого емігрували з Ірпеня до США, створив у компанії «Motorola» перший мобільний телефон [12].

Однак, сучасний етап розвитку ШІ (з 2020-х років) характеризується стрімкою інтеграцією великих мовних моделей, автоматизованих аналітичних систем та інтелектуальних рішень зокрема у сфері міжнародних відносин. Технологічні інновації, передусім ШІ, революціонізують стратегії політичних акторів. Аналіз великих обсягів даних дозволяє краще розуміти виборчу базу та настрої громадськості, що дає змогу політичним партіям та кандидатам персоналізувати свої кампанії [13].

Крім того, ШІ активно трансформує дипломатію, безпеку, глобальні стратегії та економіку, створюючи як нові можливості, так і виклики для міжнародного порядку. Автоматизація дипломатичних процесів, покращення аналітики та прогнозування кризових ситуацій сприяють підвищенню ефективності політичних рішень. Водночас використання ШІ у сфері безпеки та оборони загострює конкуренцію між державами та піднімає питання регулювання кіберзагроз [10].

ШІ однозначно сприяє автоматизації дипломатичних процесів, покращенню аналітики і прогнозування кризових ситуацій. Використання

алгоритмів у політичних рішеннях може підвищити ефективність управління та реагування на глобальні виклики. Водночас ШІ впливає на сферу безпеки та оборони, загострюючи конкуренцію між державами та піднімаючи питання регулювання кіберзагроз.

Штучний інтелект (ШІ) відіграє ключову роль у трансформації міжнародного середовища, змінюючи підходи до аналізу глобальних процесів, прийняття рішень та міждержавної взаємодії. Його здатність обробляти величезні обсяги даних і виявляти складні закономірності робить його незамінним інструментом у сфері міжнародної безпеки, дипломатії та стратегічного прогнозування. На відміну від людини, ШІ не має інтуїції у звичному розумінні, однак його алгоритми дозволяють виявляти тенденції, які могли б залишитися непоміченими у традиційних аналітичних підходах.

Попри значний потенціал, ШІ позбавлений здатності до інтуїтивного розуміння політичного контексту, що може бути критично важливим у міжнародних відносинах. Його аналіз ґрунтується на математичних моделях та обчисленнях, тоді як людський фактор враховує також дипломатичну традицію, культурні особливості та емоційний контекст переговорів.

Штучний інтелект значно змінює міжнародну комунікацію, забезпечуючи автоматизований моніторинг глобальних подій, швидке виявлення кризових ситуацій та оптимізацію процесів ухвалення рішень. Проте, незважаючи на його ефективність, ШІ не здатен повністю замінити дипломатів та політиків, оскільки він не має глибокого усвідомлення моральних та етичних наслідків своїх дій. Люди, на відміну від ШІ, можуть приймати рішення з урахуванням соціальних норм, історичних чинників та інтуїтивного передбачення можливих реакцій міжнародних партнерів.

Важливим аспектом трансформації міжнародного середовища під впливом ШІ є його застосування в оборонній сфері. Автоматизовані системи аналізу ризиків, прогнозування кіберзагроз та управління стратегічними ресурсами змінюють підходи до національної та глобальної безпеки. Проте використання ШІ у військовій сфері також породжує нові виклики, зокрема

ризики неконтрольованого ескалаційного сценарію у випадку конфлікту, про що буде детальніше розкрито в наступних розділах.

Окрім цього, ШІ сприяє розвитку нових економічних і політичних моделей взаємодії між державами. Він стає ключовим фактором у глобальному технологічному суперництві, визначаючи конкурентоспроможність країн на світовій арені. Держави, що володіють передовими ШІ-технологіями, отримують стратегічні переваги, що впливає на баланс сил у міжнародній системі.

Технологічні інновації значно розширюють масштаби політичної комунікації. Соціальні мережі, онлайн-платформи та мобільні додатки надають можливість політичним лідерам спілкуватися з великою аудиторією швидко та ефективно. Однак важливо враховувати вплив алгоритмів, які керують відображенням інформації, щоб уникнути формування інформаційних «бульбашок» та забезпечити об’єктивне сприйняття [14].

Технологічні засоби дозволяють створювати нові форми мобілізації громадськості. Від електронних петицій до краудфандингу для політичних кампаній – технології роблять участь громадськості у політичних процесах більш доступною та ефективною. Інтерактивність онлайн-платформ сприяє залученню молоді до політичних обговорень та активної участі у громадському житті.

Штучний інтелект відіграє ключову роль у трансформації міжнародного середовища, змінюючи як стратегії держав, так і глобальні політичні процеси. Він впливає на дипломатію, глобальну безпеку, економічні відносини, геополітичну конкуренцію та вирішення глобальних викликів [15].

ШІ аналізує величезні обсяги даних, включаючи новини, соціальні медіа, економічні показники та інші джерела. Це дозволяє створювати точні прогнози щодо динаміки міжнародних конфліктів, економічних тенденцій, а також впливу політичних рішень. Він використовується для моделювання

політичних сценаріїв, що дозволяє лідерам та аналітикам оцінювати можливі наслідки та обирати найкращі стратегії [15].

Системи штучного інтелекту можуть надавати політикам матеріали для аналізу та рекомендації для прийняття рішень, сприяючи розробці ефективних політичних стратегій. Це полегшує оптимізацію використання ресурсів, включаючи фінанси, енергію та природні ресурси, що є важливим для сталого розвитку та збереження довкілля. Водночас етичні та безпекові аспекти використання ШІ мають бути враховані для забезпечення стабільності та довіри до його застосування на міжнародній арені [15].

Розвиток ШІ привернув увагу теоретиків міжнародних відносин. Школа реалізму наголошує на владі, інтересах і безпеці, підкреслюючи, що штучний інтелект може впливати на збір і аналіз інформації, прийняття рішень у кризових ситуаціях, а також на військові технології та зброю. Школа лібералізму акцентує увагу на ролі міжнародних угод, дипломатії та міжнародних організацій, зазначаючи, що ШІ сприяє співпраці у вирішенні глобальних проблем, таких як зміна клімату, боротьба з хворобами та нерівність. Особливий акцент робиться на необхідності етичного регулювання розвитку ШІ з урахуванням прав та свобод людини [16].

ШІ значно впливає на дипломатію, глобальну безпеку та економіку. Автоматизовані аналітичні системи допомагають урядам і дипломатам ефективніше обмінюватися інформацією, аналізувати величезні масиви даних та взаємодіяти з громадськістю. Чат-боти та мовні моделі сприяють розвитку цифрової дипломатії, спрощуючи комунікацію між державами та міжнародними організаціями [15].

У сфері глобальної безпеки ШІ сприяє вдосконаленню систем моніторингу та прогнозування кризових ситуацій, запобіганню конфліктам і покращенню кіберзахисту. Наприклад, алгоритми ШІ аналізують дані із супутників і сенсорів для передбачення загроз та реагування на них у реальному часі. Водночас розвиток автономних бойових систем, кіберзброї та методів кібершпигунства створює нові виклики для міжнародної безпеки,

що вимагає глобального співробітництва та розробки відповідних регуляторних норм [15].

В економічному аспекті ШІ змінює традиційні бізнес-моделі та міжнародну торгівлю. Автоматизація процесів, аналіз ринкових тенденцій та розвиток електронної комерції сприяють полегшенню доступу до світових ринків. ШІ-алгоритми оптимізують логістику та управління ланцюгами постачання, що підвищує ефективність глобального бізнесу.

Глобальні виклики, такі як зміна клімату, охорона здоров’я та боротьба з пандеміями, також можуть вирішуватися за допомогою ШІ. Алгоритми аналізу великих даних допомагають прогнозувати екологічні зміни, розробляти ефективні методи лікування захворювань та сприяти міжнародному співробітництву у сфері медицини та екології [15].

ШІ також відіграє важливу роль у геополітичній конкуренції. Держави змагаються за лідерство у розробці ШІ, кібербезпеки, квантових технологій та інших стратегічно важливих сфер. Це впливає на міжнародні альянси та баланси сил, створюючи нові виклики для глобальної політики.

Прикладами використання ШІ є IBM Watson, що аналізує великі обсяги даних у медицині, Google DeepMind, який працює над розвитком когнітивних систем, Tesla Autopilot у сфері автономного водіння, а також Amazon Alexa, Siri та Google Translate, які трансформують спосіб взаємодії людей із технологіями [15].

Таким чином, штучний інтелект значною мірою змінює міжнародне середовище, посилюючи як можливості для співпраці, так і виклики, пов’язані з безпекою та регулюванням. Його розвиток вимагає створення нових механізмів глобального управління, здатних забезпечити стабільність та ефективність його інтеграції у сферу міжнародних відносин.

## 1.3. Визначення безпекового аспекту в контексті глобального розвитку

Для повного розуміння впливу штучного інтелекту на міжнародну безпеку важливо чітко визначити його можливості та обмеження на сучасному етапі розвитку. Однак дослідження цієї технології стикається з двома основними викликами. По-перше, ШІ є динамічним явищем - технології, що стали звичними, часто перестають вважатися частиною ШІ [17].

Це означає, що сам термін зберігається для найновіших досягнень і перспективних прогнозів, а не для усталених рішень. По-друге, ШІ іноді розглядається як складне та багатогранне поняття, що включає в себе численні ідеї, концепції та виклики [18].

У сфері міжнародної безпеки існує кілька підходів до визначення ШІ. Технічний підхід описує його як здатність комп'ютерних систем виконувати інтелектуальні завдання, що традиційно потребують людської участі. Це дозволяє розглядати ШІ як інструмент, що впливає на безпеку, економіку та дипломатію. Соціально-економічний підхід акцентує увагу на його здатності змінювати соціальні, економічні та політичні процеси у глобальному масштабі. Етичний підхід наголошує на необхідності дотримання моральних норм, щоб запобігти ризикам, пов'язаним із правами людини. Людино-центричний підхід фокусується на тому, як ШІ може сприяти реалізації інтересів суспільства [19].

З огляду на зростаючу роль ШІ, дипломати повинні адаптуватися до нових викликів, пов'язаних із його впливом на міжнародний порядок. Зокрема, ШІ використовується для досягнення Цілей сталого розвитку (ЦСР), але водночас породжує загрози, такі як автономні системи озброєнь (LAWS) та питання етики у військовій та політичній сферах [19].

Важливим є те, що ШІ не тільки створює нові виклики, а й розширює інструменти дипломатії. Зокрема, технології обробки текстових даних

можуть підвищити ефективність дипломатичної діяльності, зменшуючи витрати часу на аналіз документів. Проте розвиток ШІ потребує міжнародної співпраці, оскільки невеликі країни можуть мати труднощі з розробкою подібних рішень. Водночас їх доступність може сприяти балансуванню сил у міжнародних переговорах [19].

ШІ також може стати фактором глобальної конкуренції. Держави використовують його як для розвитку, так і для досягнення геополітичних цілей. Зокрема, економічна вигода від ШІ є ключовим рушієм міжнародної гонки технологій. Однак паралельно з економічними можливостями зростають і загрози безпеці, включаючи цифровий авторитаризм. Як зазначає Ніколас Райт, розвиток ШІ може змінити баланс сил між ліберальною демократією та авторитарними режимами, оскільки технології контролю дають змогу тоталітарним урядам посилювати спостереження та обмежувати права громадян [20].

Застосування штучного інтелекту у військовій та оборонній сферах привертає значну увагу, зокрема через дискусії щодо летальної автономної зброї, або так званих «роботів-вбивць». Проте спектр можливостей ШІ у цій сфері набагато ширший і охоплює логістику, кібервійну, інформаційні операції та автономні бойові системи. Штучний інтелект може відігравати важливу роль у наступальних та оборонних стратегіях, а також у підтримці військових операцій. Водночас новітні військові технології на основі ШІ можуть змінити баланс сил у світі, що потребує перегляду оборонних доктрин, стратегій фінансування та розвитку наукових досліджень [21].

Прогнозування впливу штучного інтелекту на військові системи є складним завданням. Йдеться не лише про вдосконалення технологій, а й про те, як вони інтегруватимуться у сучасні військові доктрини. Ефективність ШІ значною мірою залежить від доступу до якісних даних, прозорості алгоритмів та забезпечення конфіденційності інформації [22]. У глобальному контексті ці аспекти набувають особливого значення, оскільки технологічний

розрив між державами може впливати на їхню безпекову спроможність та геополітичний вплив.

Штучний інтелект водночас створює нові виклики та можливості. Він може загрожувати некваліфікованим масам через автоматизацію багатьох процесів, але також здатен сприяти економічному розвитку та покращенню рівня життя. Щоб ефективно використовувати потенціал ШІ, важливо мінімізувати його можливі ризики та адаптувати суспільство до нових реалій шляхом навчання та підготовки кадрів [23].

Для забезпечення глобальної стабільності необхідно створити міжнародне середовище довіри до штучного інтелекту. Формування такої довіри вимагає розробки нового суспільного договору, який, на відміну від попередніх технологічних регуляцій, має виходити за межі національних юрисдикцій. Адже екосистема ШІ охоплює широкий спектр міжнародних гравців, включаючи хмарні платформи, технологічні корпорації, державні та наддержавні організації, такі як ЄС чи НАТО. Тому ефективне регулювання ШІ потребує глобального співробітництва та координації між усіма зацікавленими сторонами [23].

Штучний інтелект здатний імітувати процеси навчання, розв’язання проблем і ухвалення рішень, які раніше були виключною прерогативою людини. Його застосування вже охоплює широкий спектр сфер – від фінансового аналізу до систем розпізнавання мовлення. Однак між швидкими обчисленнями та здатністю до прогнозування, взаємодії та розуміння намірів людини існує суттєва різниця.

Наразі ми ще далекі від створення автономних ШІ-дипломатів, які самостійно розроблятимуть міжнародні угоди та здійснюватимуть дипломатичні маневри. Важливо, щоб ухвалення ключових рішень залишалося під контролем людини, особливо в сфері безпеки.

Проте, у міру вдосконалення технологій штучного інтелекту, його роль у дипломатії та міжнародній політиці зростатиме, особливо коли ШІ почне проходити тест Тюрінга і стане практично не відрізненним від людини у

спілкуванні. Це створює ризики для глобальної безпеки, оскільки розвиток ШІ набуває характеру технологічної гонки, що може змінити баланс сил у світі [24].

Особливо важливим є потенціал штучного інтелекту у сфері моніторингу дипломатичних текстів. Завдяки алгоритмам аналізу даних можна швидко виявляти розбіжності у версіях переговорних документів, що допоможе забезпечити прозорість і точність переговорного процесу.

У складних багатосторонніх дискусіях це може стати ключовим інструментом для оцінки пропозицій різних сторін та їх відповідності міжнародним нормам. Хоча такі методи вже використовуються, вони залишаються дорогими та трудомісткими, проте інтеграція ШІ може значно прискорити та здешевити ці процеси [25].

Оскільки дипломатична практика має чітко структуровані правила та формалізовану термінологію, дипломатичні документи є ідеальним об’єктом для машинного аналізу. Використання штучного інтелекту в цьому напрямі може сприяти зміцненню глобальної безпеки, запобігаючи маніпуляціям і дезінформації, а також підвищуючи ефективність міжнародного співробітництва. В умовах сучасних глобальних викликів застосування ШІ має бути спрямоване на забезпечення стабільності та передбачуваності міжнародних відносин, з урахуванням етичних і безпекових аспектів його використання [25].

Тож, як ми вже неодноразово зазначали, технології штучного інтелекту дедалі більше інтегруються в політичну, соціальну, економічну та безпекову сфери, стаючи ключовим фактором уразливості міжнародної системи. Вони можуть впливати на громадську думку, результати виборів через поширення фейкових новин та маніпулятивного контенту в соціальних мережах, а також створювати загрози для критичної інфраструктури різних країн.

Такі нові форми конфліктів важко контролювати, що вимагає переосмислення міжнародних механізмів регулювання безпекових аспектів штучного інтелекту. Без міжнародних правових обмежень автономні системи

озброєння можуть опинитися в руках недержавних суб'єктів, зокрема терористичних організацій, що становить серйозний виклик глобальній безпеці [26].

Сьогодні боротьба держав за технологічне лідерство у сфері штучного інтелекту нагадує космічну гонку XX століття. Основними гравцями є Сполучені Штати Америки та Китай, які реалізують агресивні стратегії розвитку ШІ, що, у свою чергу, формує виклики для інших країн у визначенні їхнього місця в цифровій архітектурі світового порядку. Це спонукало міжнародну спільноту до активного розвитку правових механізмів регулювання штучного інтелекту, які мають слугувати орієнтиром для урядів та корпоративного сектору.

Концептуальну основу міжнародного регулювання ШІ закладено у «Принципах Асіломара», ухвалених у 2017 році експертною спільнотою. Один із ключових принципів зазначає, що «суперінтелект слід розвивати лише в інтересах усього людства, а не окремої держави чи організації» [26].

Аналіз міжнародної нормативної бази підтверджує пріоритет етичного підходу до розвитку ШІ, що знаходить відображення у таких документах, як резолюція Ради Європи «Технологічна конвергенція, штучний інтелект і права людини» [27], директива ОЕСР «Рекомендації Ради зі штучного інтелекту» [28] та угода ЮНЕСКО, підписана 193 країнами, що визначає спільні цінності та принципи розвитку ШІ [29].

Крім того, Велика двадцятка ухвалила «Принципи відповідального управління надійним штучним інтелектом», які формують основи міжнародної співпраці у впровадженні цих технологій [30].

Фінансово-економічна сфера також відчуває значний вплив штучного інтелекту, що змушує глобальні фінансові інституції, зокрема Міжнародний валютний фонд та Світовий банк, розробляти стратегії реагування на цифрові трансформації [31].

Штучний інтелект також є центром міжнародних дискусій щодо його використання у військовій сфері та управлінні майбутніми воєнними

конфліктами. Водночас технологія сама по собі не є простою заміною військової сили – її ефективність визначається нормативними та інституційними рамками використання. У трансатлантичному вимірі основою міжнародного регулювання ШІ є нормативно-інституційна платформа НАТО.

З огляду на зростання глобальної нестабільності та ескалацію конфліктів питання правового регулювання штучного інтелекту у сфері безпеки та оборони набуває особливої актуальності. Затверджена у 2021 році «Стратегія штучного інтелекту» НАТО визначає етичні принципи його використання у військовій сфері, окреслює загрози, пов’язані з його застосуванням супротивниками, та пропонує шляхи міжнародної співпраці для ефективного реагування на ці виклики [32].

Таким чином, розвиток технологій штучного інтелекту створює як можливості, так і нові загрози для міжнародної безпеки. Необхідність глобального регулювання цих процесів є критично важливою для збереження стабільності світового порядку та запобігання можливим конфліктам, пов’язаним із застосуванням ШІ.

Штучний інтелект стає ключовим фактором впливу на міжнародну безпеку, що змушує держави та міжнародні організації формувати відповідні стратегії його регулювання. НАТО активно працює над впровадженням ШІ у сферу безпеки та оборони, залучаючи 11 спеціалізованих підрозділів, які координують рішення держав-членів та встановлюють стандарти використання технологій у військових операціях.

Однак всередині Альянсу відсутній консенсус щодо етичних аспектів, зокрема рівня автономності бойових систем. Це пояснюється різними підходами держав-членів до регулювання ШІ [33].

Більш системний підхід до створення стандартів регулювання демонструє Європейський Союз. У межах ЄС відбувається одночасний розвиток нормативної бази як на загальноєвропейському рівні, так і в національних політиках держав-членів. Вже розроблено близько 60 програм і

планів розвитку ШІ [34]. Основним пріоритетом є встановлення етичних стандартів використання технологій. Серед ключових документів у цій сфері – «Етичні рекомендації для надійного ШІ» [35], Біла книга «Про штучний інтелект – європейський підхід до досконалості та довіри» [36], «Європейський акт про управління даними», «Акт про цифрові сервіси» та «Європейська стратегія кібербезпеки». Координацію політики у цій сфері здійснює Європейська Комісія, яка також ініціювала створення Європейського Альянсу зі штучного інтелекту – платформи, що об'єднує понад 6000 стейкхолдерів.

На інших континентах також ведеться активна робота щодо регулювання ШІ. «Стратегія цифрової трансформації для Африки (2020-2030)», ухвалена Африканським Союзом, передбачає вироблення спільної позиції щодо розвитку ШІ, створення аналітичних центрів і робочих груп для оцінки потенційних загроз та можливостей цих технологій [41]. В Азії домінуючу роль у цифровій сфері відіграє Китай, який реалізує стратегію «Цифрового шовкового шляху» [42].

Водночас Асоціація держав Південно-Східної Азії розробила «Цифровий генеральний план» до 2025 року, де питання безпеки та регулювання ШІ є одним із пріоритетних напрямків. У Латинській Америці держави зосереджені на створенні власних урядових стратегій щодо ШІ, проте поки що не мають спільної наднаціональної політики.

Міжнародне співробітництво у сфері ШІ також набирає обертів, і важливу роль у цьому процесі відіграють глобальні організації. Проблематикою безпеки та регулювання ШІ займаються спеціалізовані групи, такі як Міжвідомча робоча група ООН і Робоча група з управління штучним інтелектом ОЕСР. Найперспективнішими для координації глобальних безпекових питань ШІ є багатосторонні платформи, які залучають уряди, бізнес, науковців та громадськість. Наприклад, Глобальне партнерство зі штучного інтелекту об'єднує 24 держави та ЄС з метою аналізу ризиків і розробки рекомендацій щодо надійного використання ШІ.

Світовий економічний форум також ініціював створення Глобального альянсу дій зі штучного інтелекту для координації зусиль виробників і користувачів технологій ШІ у сфері безпеки. Інший його проєкт – «Дані для спільної цілі» – залучає 25 країн і понад 80 організацій для розробки стандартів використання даних у сфері національної та міжнародної безпеки.

Попри активний розвиток міжнародних ініціатив, ключовими проблемами залишаються відсутність глобальної організації, що координувала б регулювання ШІ, а також недостатня юридична обов'язковість міжнародних нормативних документів. Більшість рекомендацій, що ухвалюються міжнародними структурами, не мають зобов'язального характеру, що обмежує їхній вплив на національну політику держав. Це створює ризики односторонніх рішень у сфері безпеки ШІ, що може спричинити зростання технологічної нерівності та нових форм цифрових загроз. Відтак, важливим завданням глобальної спільноти є формування ефективної системи міжнародного регулювання безпекових аспектів штучного інтелекту.

Тож, підсумовуючи, основні виклики глобального регулювання ШІ можна представити у табл.1.3

Таблиця 1.3

**Основні виклики глобального регулювання ШІ**

| Виклик | Опис |
|---|---|
| **Відсутність імперативних норм** | Більшість міжнародних регуляторних актів носять рекомендаційний характер, що дозволяє державам їх ігнорувати. |
| **Нестача профільних органів** | Відсутність спеціалізованих структур у міжнародних організаціях призводить до несистемного управління розвитком ШІ. |
| **Обмежені ресурси міжнародних організацій** | На відміну від держав, які вкладають ресурси в ШІ, міжнародні організації виконують переважно аналітичні та консультативні функції. |
| **Перевага національних стратегій** | Держави, такі як США і Китай, мають сильні національні політики щодо ШІ, що послаблює глобальну координацію. |

*Джерело: розроблено автором на основі власних узагальнень*

Отже, штучний інтелект стає ключовим фактором, що впливає на міжнародну безпеку, створюючи як нові можливості, так і значні виклики. Його розвиток змінює баланс сил у світі, сприяє трансформації дипломатії, економіки, військової сфери та соціальних процесів. Водночас використання ШІ породжує загрози, такі як автономні бойові системи, цифровий авторитаризм і маніпулювання інформацією. Це вимагає комплексного підходу до регулювання технології на міжнародному рівні, зокрема через співпрацю держав, міжнародних організацій та корпорацій. Забезпечення етичного використання ШІ, розробка правових норм і глобальних стандартів є критично важливими для підтримання стабільності світового порядку та запобігання потенційним конфліктам.

# РОЗДІЛ ІІ
# ШТУЧНИЙ ІНТЕЛЕКТ І ВИКЛИКИ В ГЛОБАЛЬНІЙ БЕЗПЕЦІ

## 2.1. Кібербезпека та загрози цифровій інфраструктурі: роль ШІ

Сучасний світ стикається з безпрецедентним зростанням кіберзлочинності. З кожним роком кількість атак на цифрові системи невпинно збільшується, а їх складність досягає нового рівня. Хакери вдосконалюють свої методи та активно застосовують передові технології для реалізації загроз. У відповідь на ці виклики необхідно шукати ефективні механізми захисту, і одним із ключових інструментів у цій боротьбі є штучний інтелект.

ШІ дедалі більше використовується для виявлення загроз, аналізу аномалій у цифрових мережах та швидкого ухвалення рішень у режимі реального часу. Основна перевага цих алгоритмів - здатність аналізувати великі обсяги даних, виявляючи закономірності та підозрілу активність набагато швидше, ніж людина. ШІ діє за принципом OODA («спостерігай, орієнтуйся, вирішуй, дій»), що дозволяє йому оперативно реагувати на загрози та запобігати потенційним атакам [40].

Ще в 1980-х роках почали з’являтися перші системи кібербезпеки на основі алгоритмів, що працювали за заданими правилами. Однак справжній прорив став можливим завдяки стрімкому розвитку машинного навчання та нейромереж у 2000-х. Сьогодні ж штучний інтелект відіграє ключову роль у захисті цифрової інфраструктури.

Штучний інтелект став двосічною зброєю: з одного боку, він є надійним інструментом кіберзахисту, а з іншого – потужним ресурсом у руках зловмисників. Хакери швидко адаптували алгоритми ШІ для здійснення атак, зокрема:

- автоматизованого пошуку вразливостей у системах та обходу засобів захисту;

- розширеного фішингу з використанням персоналізованих атак;

- створення дипфейків для маніпуляцій і шахрайства;

- атак на ШІ-системи через «отруєння даних»;

- автоматизованої розробки шкідливого програмного забезпечення.

Ці загрози стимулюють кібербезпеку швидко розвиватися, впроваджуючи новітні алгоритми ШІ для аналізу загроз, оцінки ризиків та нейтралізації атак у режимі реального часу. Інтелектуальні системи стають основою захисту корпоративних мереж, банківських платформ, урядових ресурсів та критичної інфраструктури.

Кіберзлочинність має безпрецедентний вплив у різних сферах, і прогнозується, що її загальна вартість зросте до 10,5 трильйонів доларів у 2025 році.

У сучасну цифрову епоху кібербезпека стала важливішою, ніж будь-коли, адже бізнес-лідери прагнуть випереджати загрози в умовах постійних змін. Як і в багатьох інших галузях, штучний інтелект відіграватиме дедалі важливішу роль у сфері кіберзахисту [41].

Очікується, що до 2027 року ринкова вартість ШІ у сфері кібербезпеки досягне 46,3 мільярда доларів. Використання штучного інтелекту в кібербезпеці надає компаніям значні переваги, забезпечуючи ефективні інструменти для протидії загрозам та адаптації до нових викликів. Оскільки кіберзагрози стають дедалі складнішими й постійно змінюються, організації активно інвестують у нові технології, щоб уникнути фінансових втрат і репутаційних ризиків [42].

У 2020 році глобальні збитки від кіберзлочинності оцінювалися майже в один трильйон доларів, а середня вартість одного злому становила 4,27 мільйона доларів. Незважаючи на зусилля компаній щодо посилення захисту, зловмисники постійно знаходять нові способи проникнення в навіть найзахищеніші системи.

Швидке зростання ринку ШІ у сфері кіберзахисту підтверджують дослідження: згідно з даними Spherical Insights, у 2022 році глобальний ринок ШІ для кібербезпеки оцінювався у $15,25 млрд, а до 2032 року прогнозується його зростання до $96,81 млрд. Середньорічний темп зростання (CAGR) становитиме близько 20%, що підтверджує значущість цієї технології [40].

Через декілька років ШІ стане невід'ємною частиною системи цифрової безпеки. Його алгоритми допоможуть не лише виявляти та зупиняти атаки, а й прогнозувати потенційні загрози, забезпечуючи більш надійний рівень кіберзахисту. У такому динамічному середовищі компанії, що активно впроваджують ШІ у свої системи безпеки, отримають значну перевагу перед зловмисниками. Значення штучного інтелекту (ШІ) у сфері кібербезпеки продовжує зростати, адже цифрова інфраструктура постійно стикається з новими загрозами. Завдяки алгоритмам машинного навчання та нейромережам ШІ відіграє ключову роль у захисті інформаційних систем, виявленні атак і мінімізації ризиків. Розглянемо основні напрямки застосування ШІ для забезпечення безпеки цифрових середовищ.

ШІ здатний обробляти та аналізувати величезні обсяги даних, включаючи логи подій, сповіщення систем безпеки, результати аудиту та звіти про інциденти. Завдяки використанню алгоритмів машинного навчання, системи на основі ШІ можуть виявляти патерни, кореляції та аномалії, що сигналізують про потенційні загрози, злам або вразливості. Такий аналіз відбувається в десятки разів швидше й ефективніше, ніж при традиційних методах обробки інформації.

Окрім того, ШІ використовується для ідентифікації спроб несанкціонованого доступу до цифрових систем. Основними методами є розпізнавання сигнатур та евристичний аналіз. Перший підхід базується на порівнянні підозрілих дій із відомими патернами атак, а другий – на виявленні відхилень у поведінці користувачів і систем. Окрім цього, штучний інтелект контролює потоки мережевого трафіку, аналізуючи

взаємодію між пристроями, сервісами та користувачами, що дозволяє вчасно виявляти потенційні загрози [40].

Однією з проблем сучасних систем кібербезпеки є велика кількість хибних сповіщень, що можуть перевантажувати фахівців та знижувати ефективність реагування. Завдяки ШІ система аналізує сигнали загроз, виключаючи ті, що є безпечними, і таким чином допомагає скоротити кількість помилкових сповіщень. Використання методів статистичного аналізу та нейромереж підвищує точність оцінки ризиків і сприяє оптимізації роботи безпекових служб.

ШІ може спрощувати процес оновлення IT-інфраструктури, зокрема при впровадженні нових технологій, переході в хмарне середовище або інтеграції різних систем. Автоматизовані алгоритми аналізують конфігурацію та налаштування, виявляють потенційні конфлікти, оцінюють сумісність і продуктивність систем. Це значно прискорює процес модернізації та зменшує ймовірність появи вразливостей.

Штучний інтелект дозволяє аналізувати великі обсяги даних з метою прогнозування потенційних атак та вразливостей. Завдяки класифікації та кластеризації інформації, системи ШІ можуть створювати профілі загроз, аналізувати попередні випадки атак і формувати ефективні стратегії кіберзахисту. Такий підхід дозволяє запобігати інцидентам ще до їхнього виникнення.

Сучасні інструменти ШІ здатні автоматично аналізувати вразливості, які раніше потребували ручної перевірки експертів. Окрім цього, алгоритми можуть навчатися на основі нових типів атак, що дозволяє покращувати методи виявлення загроз. ШІ також здатний імітувати поведінку зловмисників, моделюючи реальні атаки для оцінки стійкості системи. ШІ дозволяє обробляти та аналізувати великі обсяги даних, включаючи сигнатури кібератак, аномальну поведінку в мережах та загрози інформаційної безпеки. Це дає змогу прогнозувати можливі атаки, виявляти

вектори загроз та оцінювати ризики для цифрової інфраструктури організацій.

Нейромережі можуть допомагати не лише у створенні надійних стратегій захисту, а й у підвищенні обізнаності персоналу з питань кібербезпеки. Крім того, ШІ може використовуватися для захисту хмарних сервісів, виявлення підробленого контенту, протидії фішинговим атакам та моніторингу аномальної активності в корпоративних мережах. Організації можуть використовувати два основні підходи для впровадження ШІ у свою кібербезпеку: застосування готових рішень від постачальників програмного забезпечення;  створення власної інфраструктури з кастомною розробкою.

Вибір оптимального варіанту залежить від кількох факторів: характеристик існуючої IT-інфраструктури, можливих загроз, бізнес-цілей та ресурсів компанії. Хоча готові рішення можуть здаватися простими у впровадженні, їх адаптація до потреб великої організації може бути складним та витратним процесом. Індивідуальна розробка систем безпеки на базі ШІ дозволяє гнучко налаштовувати інструменти відповідно до конкретних потреб бізнесу. Етапи впровадження ШІ у кібербезпеку відображені на рис.2.1


Рисунок 2.1. Етапи впровадження ШІ у кібербезпеку

*Джерело: розроблено автором на основі [40]*

З розвитком цифрових технологій кібербезпека стала одним із ключових викликів у всьому світі. Кількість та складність кіберзагроз зростають, що змушує загалом вдосконалювати свої захисні механізми. Штучний інтелект (ШІ) відіграє значну роль у зміцненні кібербезпеки, автоматизуючи процеси аналізу загроз, виявлення аномалій та реагування на атаки. Водночас, його застосування супроводжується певними ризиками, такими як помилкові спрацьовування та потенційне використання зловмисниками.

Штучний інтелект використовується для аналізу великих обсягів даних у режимі реального часу, що дозволяє швидко ідентифікувати підозрілі дії. За допомогою алгоритмів машинного навчання можна виявляти шкідливе програмне забезпечення, визначати шаблони атак та передбачати потенційні вектори загроз. Автоматизований аналіз значно зменшує людський фактор у

кібербезпеці, оскільки більшість атак відбувається через людські помилки або недбалість [43].

В табл. 2.1. наведений розроблений нами SWOT-аналіз використання ШІ в кібербезпеці.

Таблиця 2.1

**SWOT-аналіз використання ШІ в кібербезпеці**

| **Сильні сторони (Strengths)** | **Слабкі сторони (Weaknesses)** |
|---|---|
| Автоматизоване виявлення загроз | Хибні спрацьовування системи |
| Аналіз великих обсягів даних у реальному часі | Високі витрати на впровадження |
| Мінімізація людського фактора | Недостатня кількість фахівців |
| Прогнозування атак та адаптація до нових загроз | Проблеми з конфіденційністю |
| Захист кінцевих точок | Можливість використання ШІ хакерами |
| **Можливості (Opportunities)** | **Загрози (Threats)** |
| Розвиток нових технологій безпеки | Використання ШІ у кібератаках |
| Покращення нормативного регулювання | Зростаючий рівень складності атак |
| Інтеграція ШІ в хмарні рішення | Ризик витоку конфіденційних даних |
| Впровадження передбачувальної аналітики | Регуляторні обмеження |
| Створення більш ефективних стратегій реагування | Дефіцит спеціалістів для управління ШІ |

*Джерело: створено автором на основі власних узагальнень*

Тож, ми може виділити основні переваги застосування ШІ в кібербезпеці:

- швидкість реагування – ШІ здатний миттєво аналізувати великі обсяги даних та оперативно виявляти загрози;

- автоматизація – зменшує потребу у ручному моніторингу та аналізі, скорочуючи час реагування;

- оптимізація ресурсів – допомагає компенсувати нестачу фахівців, автоматизуючи ключові процеси;

- підвищена точність – мінімізує кількість хибних тривог, покращуючи ефективність безпекових команд;

- прогнозування загроз – аналіз історичних даних дозволяє прогнозувати потенційні атаки;

- контроль безпеки пристроїв – забезпечує захист кінцевих точок, що підключаються до мережі.

Отже, можна зробити висновок, що з розвитком технологій штучного інтелекту його роль у кібербезпеці стає дедалі важливішою. Використання машинного навчання та алгоритмів автоматизації сприяє швидкому виявленню вразливостей, скорочуючи витрати та ризики, пов'язані з цифровою безпекою.

Проте окрім переваг є на ряду і виклики впровадження ШІ в кібербезпеку:

- хибні спрацьовування – можливі помилкові ідентифікації безпечної активності як загрози;

- зловмисне використання – хакери можуть застосовувати ті ж технології для посилення атак;

- конфіденційність даних – обробка великих масивів інформації вимагає суворих заходів захисту;

- високі витрати -–розробка та підтримка ШІ-систем потребує значних інвестицій;

- брак спеціалістів – для ефективного використання технологій необхідні кваліфіковані кадри, яких не вистачає.

Тож, як ми бачимо штучний інтелект суттєво підвищує рівень захисту цифрових екосистем, проте його впровадження потребує ретельного підходу та вирішення низки викликів.

Отже, використання штучного інтелекту у кібербезпеці є перспективним напрямом, що дозволяє ефективно ідентифікувати загрози та підвищити рівень захисту інформаційних систем. Проте його впровадження пов’язане з певними викликами, такими як проблеми конфіденційності, високі витрати та можливість використання ШІ зловмисниками. Для досягнення максимального ефекту необхідно розвивати нормативну базу, навчати фахівців та впроваджувати нові методи аналітики даних. ШІ не тільки змінює сучасний підхід до кібербезпеки, але й відкриває нові горизонти для захисту інформаційних ресурсів у майбутньому.

## 2.2. Ризики використання ШІ у військовій сфері: автономні системи зброї

Штучний інтелект стає невід'ємною частиною військових стратегій у всьому світі, що супроводжується зростанням його застосування в оборонному секторі та значними інвестиціями. Згідно з прогнозами, до 2031 року глобальний ринок військового ШІ досягне приблизно 21,7 млрд доларів США, а до 2032 року – 24,7 млрд доларів США, демонструючи середньорічний темп зростання 12,4% у період 2024–2033 років [44].

На саміті REAIM уряди 54 країн, включаючи держави G7 і Україну, дійшли згоди щодо спільної декларації, спрямованої на регулювання норм «м'якого» міжнародного права для забезпечення відповідального використання ШІ у військовій сфері [45].

ШІ має значний потенціал у військових технологіях завдяки можливості розпізнавання об'єктів і звуків, аналізу мови та автономного навчання. У звіті NATO Science & Technology Organization окреслено основні напрями впливу ШІ на обороноздатність держав [46]:

- C4ISR (командування, управління, зв'язок, комп'ютерні технології, розвідка, спостереження та рекогносцировка) – використання автономних бойових систем із ШІ допоможе виконувати завдання, які є небезпечними, трудомісткими або дорогими, в той час як інтеграція ШІ сприятиме покращенню інформаційного управління, соціального аналізу, картографування та підтримки прийняття рішень щодо цілей;

- озброєння та ефективність його застосування – ШІ допоможе у визначенні оптимальної траєкторії, ухиленні від зіткнень, виборі озброєння, оцінці бойових пошкоджень та координації дій.

- безпілотні системи (UxV) та зброя майбутнього – автономні дрони та озброєння нового покоління отримають розширені можливості завдяки ШІ, що покращить планування місій, координацію безпілотників та допомогу операторам;

- планування військових операцій – аналітичні можливості ШІ сприятимуть довгостроковому плануванню, оцінюванню складних факторів та прогнозуванню наслідків військових дій.

Дослідження застосування ШІ у військовій сфері дозволили нам виокремити вісім основних напрямів його впливу (див.рис.2.2) [47].


Рисунок 2.2. Сфери застосування ШІ у військовій галузі

*Джерело: створено автором на основі власних узагальнень*

Тож, тепер розглянемо детальніше кожну зі сфер застосування ШІ у військовій сфері.

1. Національна безпека та боротьба з тероризмом. Застосування ШІ у сфері безпеки сприяє ефективному аналізу великих обсягів текстової, графічної, аудіо та відеоінформації, що допомагає виявляти потенційні загрози та формувати доказову базу для протидії злочинності. Вдосконалені інструменти ШІ підсилюють спроможність правоохоронних органів аналізувати злочини завдяки швидкому доступу до даних та їх інтелектуальній обробці.

Ефективна обробка інформації можлива завдяки поєднанню таких технологій, як аналіз великих даних (Data Mining), машинне навчання (ML), онлайн-аналітика (OLAP), нейронні мережі, розпізнавання образів, обробка природної мови (NLP) та прогнозне моделювання. Використання генетичних

алгоритмів також довело свою ефективність у завданнях оптимізації та моделювання.

Інтеграція цих технологій у системи аналітики критичної інфраструктури підвищує готовність до надзвичайних ситуацій, покращує обмін інформацією та координацію під час криз. Це сприяє швидкому реагуванню, ранньому виявленню загроз і запобіганню катастрофічним подіям.

2. Військова логістика. Штучний інтелект сприяє оптимізації військової логістики, забезпечуючи швидке ухвалення рішень щодо транспортування озброєння, амуніції, продовольства та зв'язку. Ефективне управління логістичними процесами є критично важливим для успіху військових операцій, оскільки охоплює своєчасне постачання, ремонт і зберігання військової техніки та ресурсів.

Через динамічні зміни умов війни управління великими потоками даних потребує гнучких рішень та аналізу ризиків, адже логістичні помилки можуть мати серйозні наслідки. Автоматизація та застосування ШІ в управлінні ланцюгами постачання дозволяють впорядковувати великі масиви інформації та ідентифікувати підозрілих постачальників [48]. Військові логістичні системи поступово інтегрують ШІ, що покращує гнучкість і швидкість процесів, частково замінюючи людський фактор.

3. Відеоспостереження. Використання ШІ у військових системах відеоспостереження значно підвищує точність і ефективність розвідки. Камери з розпізнаванням об'єктів та алгоритмами глибокого навчання (DL) дозволяють ідентифікувати цілі, обробляючи зображення та відео у режимі реального часу. Українська система Griselda використовує ШІ для аналізу даних з безпілотників, супутників, соцмереж та ворожих баз, що дозволяє створювати інтерактивну карту бойових дій [49].

Інтеграція відеоспостереження у військові дрони та роботизовані системи забезпечує автоматичне наведення та розпізнавання об'єктів за допомогою комп'ютерного бачення, ML та DL. Це дає змогу операторам

швидко ідентифікувати цілі та коригувати траєкторії безпілотників. Такі технології також використовуються для виявлення підводних мін та інших загроз.

ШІ відіграє ключову роль у розпізнаванні воєнних злочинців, аналізуючи цифрові зображення та використовуючи алгоритми розпізнавання облич. Системи відеоспостереження можуть каталогізувати дані за додатковими метаданими, такими як стать, колір волосся чи аксесуари, що покращує точність ідентифікації. Технологія Advanced Perimeter Detection (APD), заснована на алгоритмах глибокого навчання, адаптується до змін у середовищі, покращуючи виявлення людей і транспорту та зменшуючи хибні спрацьовування [50].

Дрони з ШІ також використовуються для координованих атак «роєм», знищення ППО противника та викривлення радіолокаційних сигналів. Завдяки аналізу розвідданих та алгоритмам NLP, системи на кшталт Griselda можуть швидко знаходити важливу інформацію у текстових даних, що робить їх незамінними у військовій аналітиці.

4. Кібербезпека. З огляду на високі ризики витоків даних у військових мережах, ШІ відіграє ключову роль у забезпеченні кібербезпеки. Він допомагає ідентифікувати шкідливе програмне забезпечення, аналізує поведінку мережі, виявляє аномалії та попереджає кібератаки ще до їх активного впливу [49].

ШІ автоматично аналізує електронні листи та файли на ознаки фішингу, що дозволяє виявляти нові шкідливі програми, які можуть залишатися непоміченими для традиційних антивірусів. Розумні агенти на основі ШІ оптимізують перевірки відповідності нормам кібербезпеки та допомагають командам зосередитися на серйозних загрозах [51].

Зловмисники постійно вдосконалюють методи атак, тому використання XDR (розширеного виявлення і реагування) разом із SOC та SIEM дозволяє в режимі реального часу моніторити, аналізувати та нейтралізувати потенційні кіберзагрози [52]. Хмарні технології XDR за допомогою ШІ підвищують

точність виявлення загроз, а також забезпечують масштабованість та автоматизацію захисту.

На відміну від традиційних антивірусів, ШІ не лише розпізнає відомі сигнатури шкідливих програм, а й аналізує поведінку системи, виявляючи навіть невідомі загрози. Це значно посилює захист конфіденційних даних і мінімізує ризики злому. Попри можливі недоліки, партнерство між людьми та ШІ формує більш надійну систему кібербезпеки у військовій сфері.

5. Симулятори для навчання військових. Симуляції на основі ШІ створюють реалістичне середовище для військових тренувань, дозволяючи відпрацьовувати бойові сценарії та розвивати необхідні навички. Інтелектуальні тренажери імітують складні ситуації, забезпечуючи глибокий аналіз дій військовослужбовців. Такі симулятори особливо поширені у підготовці бойових льотчиків, адже традиційні методи не завжди дозволяють ефективно моделювати непередбачувані ситуації під час польоту.

Завдяки ШІ та ML, пілотні тренажери відтворюють реалістичні сценарії, адаптуючись до дій користувача в режимі реального часу. Наприклад, система Air-Guardian, розроблена MIT CSAIL, аналізує напрямок погляду пілота та формує карти помітності, що допомагають заздалегідь виявляти потенційні загрози [53].

Ведуться дослідження щодо створення навігаційних систем на основі ШІ, які не залежать від супутників, що можуть бути виведені з ладу. Альтернативна технологія використовуватиме магнітні поля Землі, дозволяючи системам навчатися розрізняти природне магнітне випромінювання та сторонні електромагнітні сигнали.

Перспективи ШІ в симуляторах виходять за межі авіації, охоплюючи різні види військової робототехніки. Завдяки адаптивності та наскрізному навчанню такі системи покращують кооперативне керування та підготовку військових до реальних бойових умов.

6. Роботи зі ШІ на полі бою. На відміну від автономних транспортних засобів, бойові роботи зі ШІ зосереджені на виконанні військових завдань,

ідентифікуючи, відстежуючи та знищуючи цілі з мінімальним втручанням людини. Це підвищує ефективність операцій і знижує ризики для військових.

Українські автоматичні турелі ТГП і Wolly від DevDroid дистанційно керують зброєю та використовують комп'ютерний зір для виявлення ворога на відстані до 1000 м. Вони можуть працювати як у ручному, так і в автоматичному режимах, а оператори залишаються в безпеці на відстані до 100 м.

Іншим прикладом є робопес Spot від Boston Dynamics, що допомагає розміновувати небезпечні території. Він оснащений камерами та датчиками для автономного пересування й розпізнавання загроз. Spot застосовувався для розмінування в Україні, виконуючи завдання без ризику для саперів [54].

Технології ШІ також використовуються у «розумній» зброї. Наприклад, гвинтівка Tracking Point з автоматичним прицілом розпізнає ціль, аналізує 16 факторів (температура, вітер, віддача тощо) та здійснює постріл лише при ідеальному наведенні.

Хоча повністю автономна зброя ще не застосовується на полі бою, армії різних країн активно розробляють і впроваджують роботизовані бойові системи, що перевершують застарілі технології завдяки своїй точності та ефективності.

7. Медична допомога на полі бою. Захист здоров'я солдатів на полі бою є ключовим завданням, а технології ШІ значно підвищують ефективність медичної допомоги. Через обмежену доступність медиків і складність сортування поранених роботизовані системи на основі ШІ можуть евакуювати постраждалих у безпечні місця для надання допомоги [55].

ШІ сприяє прийняттю рішень у військовій медицині, зокрема щодо сортування поранених, визначення пріоритетів евакуації та розподілу ресурсів. Використання аналізу зображень, голосових даних і біометричних показників у реальному часі допомагає лікарям швидше оцінювати стан пацієнтів. Це дозволяє ухвалювати точніші рішення, ніж при візуальній оцінці стану людини [55].

Поєднання ШІ з роботизованими хірургічними системами відкриває можливості для дистанційних медичних втручань у бойових умовах. Автоматизовані платформи можуть надавати консультації, контролювати життєві показники та навіть виконувати складні операції, коли негайна евакуація неможлива.

Попри великий потенціал, ефективне впровадження ШІ у військову медицину потребує розвиненої інфраструктури великих даних і автоматизації медичних записів. У майбутньому медичний ШІ може допомагати у діагностиці, моніторингу пацієнтів і виборі оптимальних методів лікування важкопоранених військових [55].

8. Автономні та напівавтономні транспортні засоби. До військових автономних і напівавтономних транспортних засобів належать безпілотні наземні, повітряні, підводні та космічні апарати. Наприклад, підводний човен Ghost Shark від Anduril, оснащений операційною системою Lattice, використовує комп’ютерне зір і машинне навчання для автономної навігації. Його прототип Dive-LD здатний занурюватися на глибину до 6000 м і працювати безперервно до 10 днів, що значно перевершує можливості підводних човнів з екіпажем.

Іншим прикладом є безпілотний бойовий літак Loyal Wingman від Boeing, що працює у зв’язці з пілотованими винищувачами. ШІ аналізує дані з сенсорів, оцінює бойову обстановку та допомагає у прийнятті рішень у режимі реального часу. Літак також оснащений системами радіоелектронної боротьби для виявлення та придушення ворожих комунікацій і радарів. Впровадження ШІ у військову авіацію значно покращує ситуаційну обізнаність і точність виконання бойових завдань [56].

Безпілотні транспортні засоби використовують різні методи ШІ, зокрема RNN, LSTM та Reinforcement Learning (RL), що дозволяє адаптуватися до динамічних умов та оптимізувати маршрути. Комп’ютерний зір (CV) у БПЛА забезпечує розпізнавання цілей, прогнозування траєкторій та автоматичне наведення. Завдяки ШІ безпілотники можуть ефективніше

контролювати запаси, координувати ресурси та мінімізувати витрати, підвищуючи ефективність військових операцій [57].

Отже, на нашу думку використання штучного інтелекту у військовій сфері відкриває нові можливості для підвищення ефективності бойових операцій, покращення логістики, розвідки та кібербезпеки. Однак активне впровадження автономних систем зброї супроводжується значними ризиками, які викликають серйозні етичні, правові та безпекові питання.

Головною загрозою є відсутність людського контролю над автономними бойовими системами, що може призвести до неконтрольованих дій, зокрема випадкових атак на цивільні об'єкти чи порушень міжнародного гуманітарного права. Навіть найсучасніші алгоритми розпізнавання не гарантують безпомилкового визначення цілей, що створює ризик фатальних помилок.

Ще одним викликом є можливість кіберзломів і маніпуляцій автономними системами. У разі успішної атаки противник може перехопити контроль над бойовими роботами або спотворити їхні алгоритми, що загрожує катастрофічними наслідками. Крім того, гонка озброєнь у сфері військового ШІ може призвести до дестабілізації глобальної безпеки, оскільки країни, прагнучи технологічної переваги, можуть нехтувати питаннями регулювання.

Попри потенціал ШІ у військовій галузі, міжнародне співтовариство повинне встановити чіткі норми щодо його використання, щоб запобігти неконтрольованому розвитку автономної зброї. Регулювання на рівні ООН, посилення відповідальності за прийняття рішень і збереження людського контролю над системами бойового ШІ – ключові кроки для зменшення ризиків та забезпечення стабільності у сфері оборонних технологій.

## 2.3. Етичні дилеми застосування ШІ в системах безпеки

Штучний інтелект (ШІ) є ключовим компонентом сучасних систем безпеки, поєднуючи програмне та апаратне забезпечення для аналізу загроз та управління ризиками. Основою таких систем є алгоритми машинного навчання, зокрема штучні нейронні мережі (ШНМ), що моделюють людський мозок та використовують зважені зв'язки між нейронами. Завдяки цим технологіям ШІ здатний виявляти складні закономірності у великих масивах даних, що робить його ефективним інструментом у сфері безпеки. Однак, використання ШІ в цій галузі породжує низку етичних дилем, які потребують глибокого аналізу та регулювання [57].

Тож, для початку пропонуємо виділити основні етичні дилеми використання ШІ, які відображені на рис.2.3.

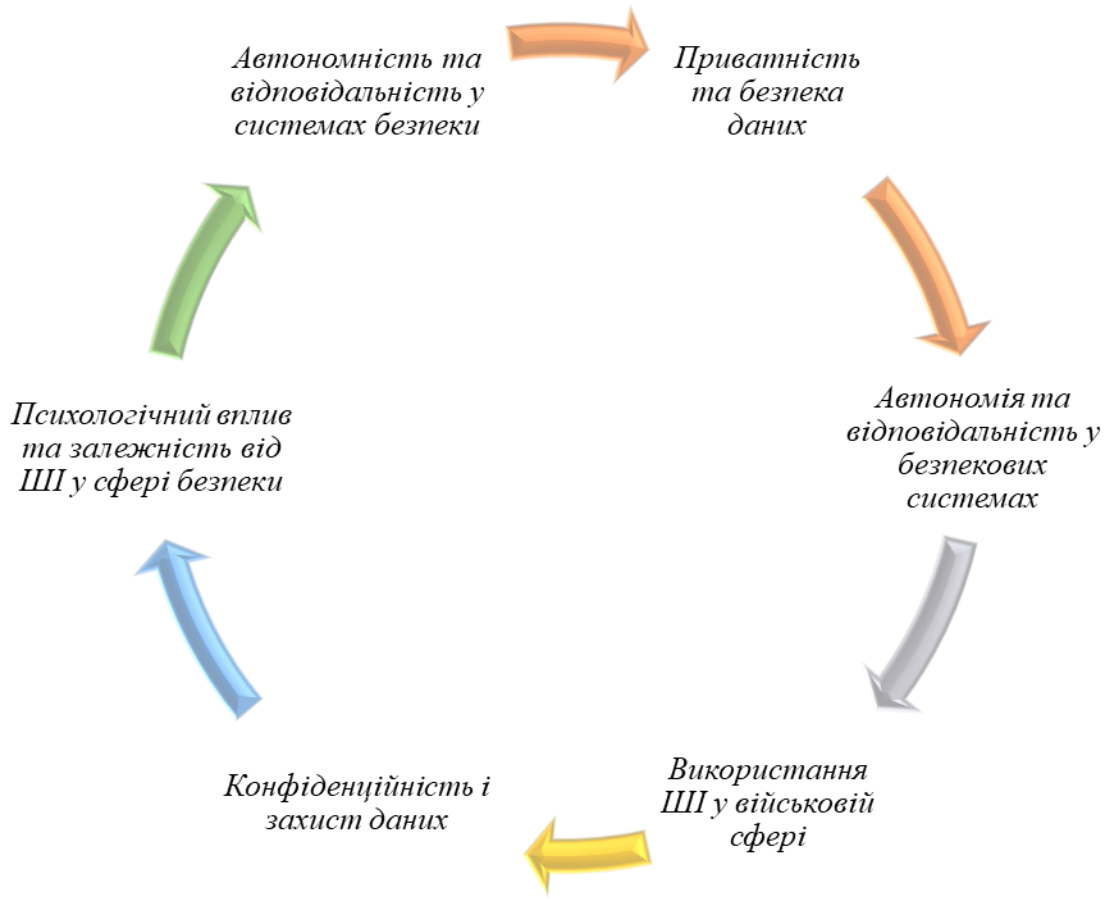


Рисунок 2.3. Основні етичні дилеми використання ШІ

*Джерело: створено автором на основі власних узагальнень*

- Приватність і безпека даних – для ефективного функціонування систем безпеки на основі ШІ потрібні великі обсяги інформації, зокрема біометричні дані, записи з камер спостереження, геолокаційні дані та фінансові транзакції. Належний захист цих даних є критично важливим, адже витоки чи зловмисний доступ можуть призвести до серйозних наслідків – від порушення приватності до фінансових злочинів. Крім того, навіть анонімізовані дані можуть бути повторно ідентифіковані за допомогою додаткових інформаційних джерел, що ставить під загрозу конфіденційність користувачів [58].

Впровадження ШІ в державні структури, відповідальні за національну безпеку, може створювати ризики надмірного стеження за громадянами. Наприклад, у квітні 2023 року група інженерів Samsung випадково передала конфіденційну інформацію в ChatGPT, намагаючись покращити власний код. Це призвело до перегляду політики безпеки компанії та обмеження використання ШІ у внутрішніх процесах. Такий випадок ілюструє, як безконтрольне використання інструментів штучного інтелекту може стати загрозою для конфіденційності, що особливо важливо для державних установ, які працюють з критично важливими даними [59].

- Автономія та відповідальність у безпекових системах – одна з головних етичних проблем у сфері безпеки – це автономія рішень, які приймають системи ШІ. Алгоритми можуть аналізувати величезні обсяги інформації та діяти без прямого втручання людини, що підвищує ефективність, але водночас створює ризики. Наприклад, автономні дрони можуть самостійно ідентифікувати цілі та завдавати удари, а системи розпізнавання осіб – визначати потенційних злочинців. Проте, виникає питання: хто несе відповідальність за помилки таких систем? Якщо автономний ШІ приймає невірне рішення, хто буде відповідальний – розробник алгоритму, оператор системи чи урядова структура, що його впровадила? [60].

Для розв’язання цього питання необхідно чітко визначити розподіл відповідальності. Юридичні та етичні аспекти застосування ШІ в безпеці потребують детального аналізу та розробки нормативних актів, які гарантуватимуть прозорість процесів прийняття рішень [60].

Окрім того, автономні системи, що використовуються у сфері безпеки, повинні бути підзвітними суспільству. Недостатня прозорість алгоритмів може спричинити випадки неправомірного затримання, хибних звинувачень або упередженого ставлення до окремих соціальних груп. Наприклад, системи розпізнавання облич часто демонструють упередженість залежно від етнічної приналежності, що може призводити до дискримінації [59].

У сфері правосуддя та правопорядку використання ШІ повинно відповідати фундаментальним етичним принципам – справедливості, рівноправності та захисту прав людини. Важливо, щоб розробники технологій співпрацювали з юристами, етичними експертами та державними органами для створення стандартів, які регламентуватимуть етичне застосування ШІ у сфері безпеки [59].

- Використання ШІ у військовій сфері – штучний інтелект активно застосовується у військовій сфері для прогнозування загроз, аналізу бойових ситуацій та автоматизації бойових систем. Використання автономних дронів та роботизованих бойових машин ставить питання щодо моральної відповідальності за їхні дії. Зокрема, чи може машина ухвалювати рішення про застосування сили без людського контролю? Відповідно до міжнародних гуманітарних норм, право на ухвалення таких рішень повинно залишатися за людиною [57].

Тому, необхідно розробити чіткі механізми контролю за використанням автономних бойових систем, щоб уникнути випадків безвідповідального застосування сили та порушення прав людини. Також слід впровадити протоколи перевірки та тестування таких систем перед їхньою експлуатацією у реальних умовах [57].

Штучний інтелект (ШІ) відіграє все більшу роль у забезпеченні безпеки, допомагаючи прогнозувати загрози, автоматизувати аналіз даних і підвищувати ефективність роботи правоохоронних органів та державних структур. Однак, разом із цими перевагами постає низка етичних викликів, пов'язаних із конфіденційністю, автономністю систем і відповідальністю за їхні рішення. Використання ШІ у сфері безпеки вимагає чіткого регулювання, контролю та забезпечення дотримання прав людини [60].

- Конфіденційність і захист даних – системи безпеки на основі ШІ обробляють величезні обсяги даних, включаючи біометричну інформацію, записи відеоспостереження, історію переміщень і фінансові транзакції. Недостатній захист таких даних може призвести до витоків інформації, зловживань і порушення приватності громадян. Наприклад, витік даних, пов'язаний із компанією Atrium Health у 2018 році, який торкнувся майже трьох мільйонів людей, свідчить про серйозні ризики, пов'язані з обробкою конфіденційної інформації в автоматизованих системах [60].

Крім того, навіть анонімізовані дані можуть бути повторно ідентифіковані, якщо використовуються додаткові джерела інформації. Це створює можливості для масового стеження, що, у свою чергу, може суперечити основним правам людини. Саме тому важливо встановити чіткі стандарти безпеки даних та прозорі механізми їхнього використання.

Впровадження ШІ в системи безпеки також має економічні та соціальні наслідки, зокрема у сфері зайнятості. Автоматизовані системи можуть замінювати працівників, виконуючи завдання з моніторингу, аналізу загроз і управління ризиками без втручання людини. Наприклад, системи відеоспостереження з ШІ можуть автоматично розпізнавати обличчя та аналізувати поведінку осіб, зменшуючи потребу в операторських центрах спостереження. Це може призвести до скорочення робочих місць серед охоронців, операторів спостереження та аналітиків безпеки [61].

Однак, паралельно ШІ створює нові професії у сфері кібербезпеки, аналізу даних і розробки алгоритмів. Для мінімізації негативних наслідків

автоматизації необхідно інвестувати в програми перепідготовки кадрів та створювати механізми соціального захисту для працівників, які втратили роботу через автоматизацію безпекових систем.

- Автономність та відповідальність у системах безпеки – одним із найскладніших етичних викликів є питання автономного ухвалення рішень системами ШІ. Автоматизовані системи можуть самостійно оцінювати рівень загрози та ухвалювати рішення про втручання без участі людини. Наприклад, алгоритми, що аналізують поведінку осіб у громадських місцях, можуть помилково класифікувати невинних громадян як потенційно небезпечних, що може призвести до неправомірних затримань або дискримінації певних соціальних груп [61].

Ще більш суперечливим є застосування ШІ у військовій сфері. Автономні дрони та бойові системи можуть приймати рішення про застосування сили без безпосереднього контролю людини. Це створює серйозні етичні ризики, оскільки алгоритми не здатні оцінювати моральні аспекти своїх дій так, як це роблять люди. Відповідно, постає питання: хто несе відповідальність за помилки таких систем – розробники, оператори чи військове керівництво?

- Психологічний вплив та залежність від ШІ у сфері безпеки – залежність державних органів та служб безпеки від ШІ може призвести до втрати контролю над певними аспектами ухвалення рішень. Якщо автоматизовані системи стають основним джерелом аналізу загроз і управління ризиками, це може знизити роль людини у критичних ситуаціях, коли необхідне стратегічне мислення.

Також існує ризик психологічного впливу на працівників систем безпеки, які покладаються на рекомендації ШІ. Якщо алгоритми почнуть ухвалювати помилкові рішення, це може підірвати довіру до автоматизованих систем і викликати кризу відповідальності серед операторів, які більше не контролюють ситуацію в повному обсязі.

Отже, на нашу думку, враховуючи глобальний характер безпекових викликів, необхідно розробити міжнародні стандарти щодо використання ШІ у сфері безпеки. Такі регулювання повинні передбачати:

- прозорість алгоритмів – компанії та уряди повинні розкривати інформацію про те, як працюють алгоритми безпеки та які дані вони використовують;

- контроль і нагляд – незалежні органи повинні мати можливість оцінювати ефективність і справедливість систем безпеки на основі ШІ;

- захист прав людини – використання ШІ у сфері безпеки не повинно порушувати основоположні права, такі як конфіденційність, право на справедливий суд та свободу пересування.

Окрім того, важливим аспектом є гнучкість законодавчих механізмів, які повинні адаптуватися до швидких технологічних змін. Тільки за умов чіткої нормативної бази можна гарантувати, що ШІ у сфері безпеки буде розвиватися відповідально та етично, не створюючи загроз для суспільства.

У сучасному світі штучний інтелект все частіше використовується у сфері безпеки, що викликає низку етичних дилем, які потребують особливої уваги та регулювання. Однією з ключових проблем є конфіденційність та захист даних. Системи ШІ у сфері безпеки обробляють великі обсяги персональної інформації, що може призвести до порушення приватності громадян, якщо не буде впроваджено надійних механізмів контролю та безпеки даних.

Автономність ШІ у прийнятті рішень також становить серйозний виклик. Використання автоматизованих систем у правоохоронній діяльності або в сфері національної безпеки може призвести до ситуацій, коли ШІ ухвалює критично важливі рішення без безпосереднього втручання людини. Це ставить питання про відповідальність за такі рішення, а також про ризик упередженості або помилок, що можуть мати серйозні наслідки для суспільства.

Ще одним аспектом є соціальний вплив автоматизації в сфері безпеки. Використання ШІ може зменшити потребу в людському факторі, що потенційно призведе до скорочення робочих місць у правоохоронних органах, службах охорони та інших суміжних галузях. Це вимагає розробки стратегій адаптації та перекваліфікації кадрів, щоб забезпечити справедливий перехід до нових умов праці.

Проблема контролю та регулювання використання ШІ в безпекових системах також є надзвичайно актуальною. Відсутність чітких стандартів та прозорих механізмів нагляду може створити ризики зловживання технологіями, що, у свою чергу, може загрожувати правам і свободам людини. Необхідно впроваджувати жорсткі етичні принципи та правові рамки, які гарантуватимуть використання ШІ виключно в інтересах суспільства.

Для забезпечення безпеки та етичного застосування ШІ важливо розробити ефективні методи захисту даних, включаючи анонімізацію та шифрування, а також забезпечити прозорість алгоритмів та їх підзвітність. Окрім цього, необхідно навчати фахівців, які працюють із ШІ, правилам безпечного та етичного використання цих технологій.

Отже, застосування ШІ в системах безпеки несе як значні переваги, так і серйозні ризики. Лише завдяки комплексному підходу, чіткому регулюванню та суспільному контролю можна мінімізувати загрози та зробити використання штучного інтелекту справедливим, надійним і відповідальним.

# РОЗДІЛ ІІІ
# ПЕРСПЕКТИВИ ТА ШЛЯХИ МІНІМІЗАЦІЇ РИЗИКІВ ВІД ВПЛИВУ ШІ НА МІЖНАРОДНУ БЕЗПЕКУ

## 3.1. Міжнародні регуляторні механізми контролю за розвитком ШІ

Міжнародні стандарти та регуляторні заходи щодо контролю розвитку штучного інтелекту є динамічними та продовжують удосконалюватися. Як зазначено в преамбулі ключових міжнародних документів, таких як Кодекс поведінки та Керівні принципи, вони залишаються «живим документом», який постійно переглядається й адаптується до нових викликів.

Основою міжнародних регуляторних механізмів є ризикоорієнтований підхід. Це означає, що всі ключові учасники процесу – від розробників до постачальників і регуляторів – повинні систематично ідентифікувати, оцінювати та мінімізувати ризики, які можуть виникати на різних етапах розробки та впровадження систем ШІ.

Для забезпечення безпеки, надійності та відповідності міжнародним стандартам, регуляторні механізми передбачають суворі заходи тестування систем ШІ. Це включає перевірку на можливі ризики та вразливості, які можуть мати як випадковий, так і навмисний характер. Випробування мають проводитися в контрольованих умовах на різних етапах життєвого циклу системи – від початкової розробки до виходу на ринок.

Ключову роль у міжнародному регулюванні відіграє забезпечення прозорості процесів розробки. Для цього компанії повинні ретельно документувати використані набори даних, алгоритми та ухвалені рішення, а також регулярно оновлювати технічну документацію.

Завдяки комплексному підходу та міжнародному співробітництву можна ефективно регулювати розвиток ШІ, мінімізуючи його ризики та забезпечуючи відповідність технологій етичним і правовим нормам.

З метою ефективного міжнародного контролю за розвитком штучного інтелекту (ШІ) ключові регуляторні механізми спрямовані на виявлення та мінімізацію потенційних ризиків. Організації, що займаються розробкою ШІ, несуть відповідальність за впровадження належних заходів тестування, з особливим акцентом на такі загрози:

- ризики хімічного, біологічного, радіологічного та ядерного характеру – необхідність запобігати використанню ШІ для зниження бар'єрів у розробці та поширенні зброї, зокрема серед недержавних акторів;

- кібербезпека – контроль над тим, як ШІ може сприяти виявленню або експлуатації вразливостей інформаційних систем;

- загрози безпеці та здоров'ю – потенційний вплив ШІ на фізичні системи та критично важливу інфраструктуру;

- ризики самовідтворення ШІ – небезпека неконтрольованого поширення та навчання моделей;

- соціальні виклики – загрози упередженості, дискримінації, порушення конфіденційності та правових норм;

- ризики для демократичних цінностей – можливе використання ШІ для дезінформації або втручання у приватне життя;

- ефект ланцюгової реакції – загроза неконтрольованих наслідків, які можуть зачепити цілі міста, галузі або суспільства.

У рамках міжнародного регулювання передові системи ШІ підлягають моніторингу на всіх етапах життєвого циклу. Важливим аспектом є прозорість процесів розробки, що забезпечується ретельним документуванням ризиків та імплементацією механізмів для відповідального інформування про вразливості. Це передбачає створення умов для третьої сторони та користувачів повідомляти про проблеми, що може бути реалізовано через програми винагород, конкурси та спеціальні механізми звітності.

Ключовими інструментами міжнародного контролю є:

- звітування про прозорість – публікація розробниками інформації про нові релізи ШІ, їхні можливості, обмеження та потенційні ризики;

- співпраця між державами та організаціями – обмін даними для покращення загального рівня безпеки та надійності технологій;

- механізми автентифікації контенту – розробка та впровадження маркерів, таких як водяні знаки, для ідентифікації матеріалів, створених за допомогою ШІ.

Дотримання цих регуляторних принципів є необхідним для попередження незворотних наслідків використання ШІ та формування безпечного технологічного середовища. Водночас глобальне регулювання потребує подальшого розвитку: необхідні більш детальні міжнародні та національні норми, які забезпечать ефективне впровадження регуляторних стандартів у практичну діяльність. Так, хіросімський процес з ШІ став відправною точкою для створення таких механізмів, і їхня подальша імплементація є одним із ключових викликів у сфері глобального контролю за розвитком ШІ.

У 2023 році Лондон став центром глобальної дискусії щодо регулювання штучного інтелекту. Світові лідери, науковці та керівники технологічних компаній зібралися, щоб узгодити підходи до контролю розвитку цієї ключової технології. Проте, попри спільне декларування намірів щодо безпечного використання ШІ, досягти єдиної стратегії регулювання не вдалося.

На саміті окреслилися два кардинально різні підходи. Представник Meta Нік Клегґ порівняв спроби регулювання ШІ з будівництвом літака під час польоту, наголошуючи на складності й ризиках жорсткого контролю. Натомість президентка Єврокомісії Урсула фон дер Ляєн наполягала на дотриманні нового Закону ЄС про ШІ, який встановлює суворі вимоги до розробників, зокрема до прозорості та обмеження високоризикових застосувань технології [62].

Протистояння цих двох моделей регулювання – жорсткого контролю ЄС та гнучкого підходу США – стало ключовою темою глобальної дискусії. Під час саміту Великої сімки в Японії Євросоюз прагнув переконати партнерів ухвалити його підхід, але американський дипломат Натаніель Фік виступив за більш м'яке регулювання, засноване на добровільних зобов'язаннях. США наголошували на важливості інновацій та уникненні надмірного регуляторного тиску[62].

Попри розбіжності, 29 країн, включаючи Китай, США та членів ЄС, підписали міжнародну угоду про зменшення ризиків ШІ. Документ став першим кроком до глобального регулювання, але дискусії щодо жорсткості контролю тривають.

Президент Франції Емманюель Макрон також активно долучився до дискусії, організувавши зустріч у Єлисейському палаці з провідними експертами галузі, зокрема представниками OpenAI та Meta. Макрон намагався знайти компроміс між жорсткою регуляцією ЄС і необхідністю підтримки інновацій, щоб не загальмувати розвиток європейських ШІ-компаній, таких як Mistral[62].

Під час дискусії також зіткнулися два підходи: одна частина учасників, зокрема представники OpenAI, наголошувала на необхідності зосередитися на довгострокових загрозах ШІ, тоді як інші, такі як Мередіт Віттакер, наполягали на негайних заходах через вже існуючі проблеми, зокрема упередженість алгоритмів та ризики дезінформації.

Великі технологічні компанії активно намагаються вплинути на процес регулювання. Колишній гендиректор Google Ерік Шмідт і засновник LinkedIn Рід Гоффман аргументували, що надмірний контроль дасть перевагу Китаю, де ШІ розвивається в умовах централізованого державного управління. Водночас критики вказують на те, що технологічні корпорації можуть применшувати нинішні ризики ШІ, зосереджуючись лише на потенційних загрозах у майбутньому.

Питання ліцензування розробки ШІ стало одним із ключових в обговореннях. Microsoft і OpenAI підтримують ідею обмеженого доступу до створення передових ШІ-моделей, аргументуючи це необхідністю кращого державного контролю. Водночас противники такої моделі, включаючи Mozilla Foundation, вважають її способом усунення конкуренції та концентрації технології в руках кількох корпорацій.

Хіросімський процес зі штучного інтелекту (ШІ) є важливою ініціативою, започаткованою країнами «Великої сімки» (G7) під час саміту в Хіросімі у травні 2023 року. Цей процес спрямований на розвиток глобальних стандартів та принципів для забезпечення безпечного, надійного та етичного використання ШІ [63].

У рамках Хіросімського процесу були прийняті такі ключові документи:

- Декларація міністрів з технологій та цифрових питань, яка окреслює спільне бачення країн G7 щодо розвитку та регулювання ШІ;

- Хіросімське комюніке лідерів держав, що підтверджує прихильність до співпраці у сфері ШІ та встановлення міжнародних стандартів;

- Міжнародні керівні принципи для організацій, які займаються розробками передових систем ШІ, які рекомендують дотримуватися принципів надійності, відповідальності, прозорості та справедливості.

Ці документи формують основу для глобального управління ШІ та впливають на політику і практики далеко за межами країн G7. Завдяки Хіросімському процесу, міжнародне співтовариство отримало дорожню карту для обговорення та впровадження передових систем ШІ, що сприяє узгодженню підходів до регулювання та розвитку цієї технології.

Важливим аспектом Хіросімського процесу є його вплив на міжнародне співробітництво у сфері ШІ. Наприклад, Європейський Союз та Японія оголосили про співпрацю між офісом ЄС зі штучного інтелекту та Інститутом безпеки Японії, підтримуючи Хіросімський процес для просування безпечного та надійного ШІ.

Крім того, Організація економічного співробітництва та розвитку (ОЕСР) оприлюднила книгу «Хіросімський процес G7 щодо генеративного штучного інтелекту: на шляху до спільного розуміння G7 щодо генеративного ШІ», підготовлену Директоратом з науки, технологій та інновацій ОЕСР.

Отже, Хіросімський процес є ключовою ініціативою, яка сприяє формуванню міжнародних регуляторних механізмів для контролю та розвитку ШІ, забезпечуючи безпечне та етичне впровадження цієї технології у глобальному масштабі.

Тож, міжнародні регуляторні механізми контролю за розвитком штучного інтелекту (ШІ) перебувають у процесі активного формування та вдосконалення. Світова спільнота намагається знайти баланс між необхідністю жорсткого контролю та збереженням простору для технологічних інновацій.

Протистояння між підходами Європейського Союзу, який просуває суворі обмеження, та США, які виступають за м’яке регулювання на основі добровільних зобов’язань, відображає глобальну дискусію щодо найефективнішої стратегії. Хіросімський процес, започаткований країнами G7, став важливим кроком до розробки універсальних стандартів безпечного та етичного використання ШІ, що підтверджується ухваленими деклараціями та міжнародними угодами.

Для ефективного регулювання штучного інтелекту країни повинні забезпечити прозорість у розробці та впровадженні технологій, посилити механізми моніторингу ризиків і запровадити міжнародні стандарти контролю. Водночас співпраця між державами, науковцями та технологічними компаніями має відігравати ключову роль у забезпеченні надійності та безпеки ШІ.

Регулювання ШІ є не лише технічним або економічним питанням, а й глобальним викликом, що впливає на демократію, безпеку та права людини. Від вибору між жорстким контролем і відкритим підходом залежить не лише

розвиток ШІ, але й те, наскільки безпечно та справедливо ця технологія інтегруватиметься у суспільне життя.

### 3.2. Роль міжнародної співпраці у формуванні безпечного використання ШІ

Сучасний розвиток технологій ШІ вимагає належного правового регулювання, зокрема у сфері кібербезпеки. Одним із ключових питань є визначення правосуб'єктності ШІ, захисту масивів інформації та баз даних. Можна прослідкувати, що активне використання технологій розпізнавання облич, таких як Clearview AI, викликало занепокоєння щодо гарантій захисту персональних даних, особливо у воєнний час.

Наприклад, використання цього інструменту в Україні дозволило здійснити понад 100 тисяч пошукових запитів для ідентифікації воєнних злочинців, що підкреслює необхідність міжнародного співробітництва у сфері правового регулювання ШІ.

Так, у США, ЄС, Японії активно розвиваються механізми правового регулювання ШІ, що дозволяє створювати ефективні стратегії для його безпечного використання. Зокрема, у США було розроблено нову «Кіберстратегію–2023», яка враховує реалії сучасних кібероперацій та спрямована на комплексне забезпечення кібербезпеки.

Міжнародна співпраця сприяє формуванню стандартів відповідального використання ШІ. Європейський Союз ухвалив Закон про штучний інтелект (Artificial Intelligence Act), який встановлює етичні принципи, правила використання та рекомендації щодо систем автоматизованого прийняття рішень. Україна активно долучається до цього процесу, запустивши регуляторну «пісочницю» для розробників ШІ, що дозволяє інтегрувати європейські норми у національну правову систему.

Одним із важливих аспектів міжнародної співпраці є обговорення питань кібербезпеки на міжнародних платформах. Так, під час 60-ї

Мюнхенської конференції з безпеки обговорювалися загрози з боку Росії та можливості підвищення обороноздатності за допомогою ШІ. Голова Єврокомісії Урсула фон дер Ляєн наголосила на необхідності інтеграції України в стратегію воєнної промисловості ЄС, що забезпечить ефективну взаємодію у сфері оборонних технологій.

Велика Британія також відіграє значну роль у формуванні міжнародних стандартів використання ШІ. Національна стратегія штучного інтелекту Великої Британії базується на принципах безпеки, прозорості, справедливості та підзвітності. У країні функціонує понад 200 стартапів і підприємств, які працюють у сфері ШІ, а також створено спеціалізовані центри, такі як «Цифрова катапульта» (Digital Catapult), що сприяють розвитку новітніх технологій.

Міжнародна співпраця у сфері регулювання ШІ передбачає створення спеціалізованих інституцій, які координують діяльність у цій галузі. Наприклад, у ЄС діє Європейський альянс зі штучного інтелекту, що об’єднує понад шість тисяч стейкхолдерів. Крім того, Європейський парламент створив Європейську раду з питань штучного інтелекту, що займається розробкою регулятивних норм.

Загалом міжнародне співробітництво відіграє вирішальну роль у забезпеченні безпечного використання ШІ. Спільні зусилля країн сприяють розробці ефективних правових норм, що допомагають запобігати потенційним загрозам та спрямовувати розвиток ШІ у безпечне русло.

Міжнародна співпраця відіграє ключову роль у формуванні безпечного використання штучного інтелекту, особливо в умовах сучасних глобальних викликів. Одним із важливих прикладів міжнародного партнерства є підписання 12 січня 2024 року Угоди про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії та Північної Ірландії. Даний документ передбачає спільну роботу в таких напрямах, як обмін розвідувальними даними, військова та кібербезпека, а також оборонно-промислове співробітництво, що має велике значення для створення

ефективних механізмів захисту від кібератак і забезпечення безпечного використання ШІ.

У рамках реалізації цієї угоди Велика Британія надає комплексну допомогу Україні у захисті територіальної цілісності та активному стримуванні загроз. Зокрема, передбачено посилення кіберстійкості, обмін розвідувальними даними та розробку механізмів протидії зловмисним кібероперація̈м. Важливим аспектом є використання сучасних технологічних рішень у сфері захисту критичної інфраструктури та впровадження спільних протоколів реагування на кібератаки, що безпосередньо стосуються безпечного функціонування ШІ.

Окрему увагу міжнародна спільнота приділяє правовому регулюванню ШІ. Наприклад, Канада активно розвиває державну політику в цій сфері, приймаючи законодавчі ініціативи, такі як Національна стратегія ШІ та законопроєкти C-27 і AIDA, спрямовані на забезпечення прозорості, етики та відповідальності у використанні штучного інтелекту. Також Канада є співзасновником Глобального партнерства зі штучного інтелекту, що працює над мирним використанням цієї технології та запобіганням її застосуванню у військових конфліктах.

Значний внесок у міжнародне регулювання використання ШІ робить Північноатлантичний альянс (НАТО). Альянс акцентує увагу на відповідальності за поширення цифрових технологій та їх вплив на права людини. Наприклад, у межах цього підходу Україна, враховуючи міжнародні стандарти, рухається до створення власної законодавчої бази для регулювання ШІ. Особливістю цього процесу є інтеграція норм військово-адміністративного права, що враховує специфіку застосування ШІ у воєнний час.

Аналіз міжнародного регулювання ШІ представлений в табл.3.1

Таблиця 3.1

**Аналіз міжнародного регулювання ШІ**

| Країна/Організація | Ініціативи та нормативні акти | Основні напрями регулювання |
|---|---|---|
| **ЄС** | Artificial Intelligence Act | Етичні принципи, правила використання, регулювання автоматизованих рішень |
| **США** | Кіберстратегія-2023 | Кібербезпека, відповідальність за використання ШІ |
| **Канада** | Національна стратегія ШІ, законопроєкти С-27 і AIDA | Прозорість, етика, відповідальність |
| **Велика Британія** | Національна стратегія штучного інтелекту | Безпека, прозорість, справедливість, підзвітність |
| **НАТО** | Політика цифрової безпеки | Контроль поширення технологій, права людини |
| **Україна** | Концепція розвитку ШІ, Кіберстратегія | Інтеграція до стандартів ЄС, кібербезпека, правове регулювання |

*Джерело: створено автором на основі власних узагальнень*

Отже, міжнародна співпраця є важливим фактором у формуванні безпечного використання ШІ. Обмін досвідом, спільні технологічні ініціативи та правове регулювання сприяють створенню ефективних механізмів захисту від загроз, що забезпечує стабільний розвиток штучного інтелекту в глобальному масштабі.

Забезпечення безпечного використання штучного інтелекту вимагає тісної міжнародної співпраці, оскільки проблема кіберзагроз і зловживання цифровими технологіями виходить за межі окремих держав. Україна активно розвиває партнерство у сфері кібербезпеки з такими країнами, як США, Велика Британія, Німеччина, Нідерланди, Канада, Норвегія, Румунія, Японія, а також співпрацює з Європейським Союзом і НАТО, що сприяє впровадженню міжнародних стандартів і кращих практик у цій сфері.

Розвиток правового регулювання штучного інтелекту значною мірою залежить від міжнародної співпраці, особливо в умовах сучасних глобальних

викликів. Держави, спільно з бізнес-сектором та науковими установами, працюють над створенням адаптивних і ефективних правових норм, що враховують особливості розвитку та використання ШІ. Така взаємодія сприяє забезпеченню кібербезпеки, захисту прав людини та створенню стабільного цифрового простору для інноваційного розвитку.

З урахуванням світового досвіду, стратегічні напрями міжнародного співробітництва у сфері безпечного використання ШІ включають:

- координацію зусиль для розробки глобальних етичних стандартів застосування ШІ у фізичному та віртуальному середовищі;

- створення механізмів спільного реагування на кіберзагрози та недопущення використання штучного інтелекту у військових конфліктах;

- розбудову міжнародних дослідницьких центрів для підвищення стійкості до потенційних загроз цифрових технологій;

- забезпечення прозорості та підзвітності алгоритмів ШІ відповідно до фундаментальних принципів безпеки, справедливості та відповідальності;

- обмін даними та передовими практиками у сфері кібербезпеки, а також проведення спільних навчань і консультацій щодо виявлення та запобігання кібератакам;

- залучення міжнародної технічної допомоги для зміцнення інституційного потенціалу держав у сфері цифрових технологій;

- розробку глобальної нормативно-правової бази щодо регулювання штучного інтелекту, що враховуватиме ризики порушення прав людини та можливі загрози кіберзлочинності.

Міжнародна співпраця є ключовим елементом у формуванні глобальної стратегії щодо безпечного використання ШІ. Спільні зусилля держав, наукових установ, приватного сектору та громадянського суспільства сприятимуть створенню ефективного правового регулювання, що забезпечить захист прав і свобод людини та мінімізує ризики, пов’язані з розвитком цифрових технологій.

### 3.3. Стратегії зниження ризиків: технічні, політичні та соціальні аспекти

Як вже було відмічено в минулих розділах, широке використання штучного інтелекту несе в собі ризики, які можуть бути як технічними, так і соціально-політичними. До основних загроз належать кібербезпека, етичні проблеми, ризики упередженості алгоритмів, а також потенційні наслідки автоматизації для ринку праці. Для мінімізації цих викликів, на нашу думку необхідно розробити комплексні стратегії, що включають технологічні інновації, регуляторні механізми та суспільну відповідальність.

1. Технічні аспекти зниження ризиків. Одним із ключових напрямів зниження ризиків є вдосконалення технологій ШІ та впровадження надійних алгоритмів. По-перше, це передбачає створення прозорих і пояснюваних моделей ШІ (Explainable AI, XAI), які дозволяють розуміти логіку ухвалення рішень і, відповідно, контролювати можливі помилки або несподівані відхилення. По-друге, важливою є розробка механізмів виявлення та усунення упередженості в алгоритмах, що знижує ризик дискримінації в автоматизованих системах ухвалення рішень. Окрім цього, необхідно вдосконалювати методи захисту ШІ від атак, таких як Adversarial Machine Learning, які можуть спотворювати результати роботи алгоритмів.

Не менш важливим є питання кібербезпеки та захисту даних. Впровадження протоколів безпеки допомагає запобігти кібератакам, які можуть порушити роботу ШІ-систем або використати їх для зловмисних цілей. Захист персональних даних має базуватися на сучасних методах шифрування та децентралізованих моделях зберігання інформації, що мінімізує ризики витоку конфіденційних даних. Крім того, необхідний регулярний аудит ШІ-систем для виявлення потенційних уразливостей і забезпечення їх безперервного вдосконалення.

Контроль автономності та ухвалення рішень є ще одним важливим напрямом у зниженні ризиків використання ШІ. По-перше, необхідно

забезпечити людський контроль над критично важливими рішеннями, особливо в таких сферах, як медицина, правосуддя або військова справа. По-друге, важливо встановити чіткі рівні автономності ШІ, що дозволить запобігти неконтрольованій поведінці систем. Використання гібридних моделей ухвалення рішень, де ШІ виконує роль аналітичного інструменту для людини, дозволяє знизити ризики та підвищити якість ухвалених рішень.

2. Політичні аспекти зниження ризиків. Оскільки ШІ має глобальний вплив, необхідно розробляти міжнародні механізми регулювання його використання. Зокрема, це включає створення глобальних етичних норм, розроблених у межах ініціатив ООН, ЄС, НАТО та інших міжнародних організацій. Співпраця між країнами є важливою для формування єдиних стандартів використання ШІ у військовій сфері, правоохоронній діяльності та інших критичних галузях. Крім того, гармонізація національного законодавства з міжнародними стандартами дозволить забезпечити відповідальність за рішення, ухвалені ШІ.

Розвиток державної політики щодо ШІ повинен включати інтеграцію технологій у стратегії кібербезпеки, а також підтримку наукових досліджень у цій сфері. Важливим є забезпечення відкритих даних, що сприятиме розвитку етичного та безпечного ШІ. Крім того, необхідно розробити механізми відповідальності за наслідки використання ШІ та впровадити законодавчий контроль у критичних сферах, таких як медицина, фінанси та правосуддя. Одним із ключових кроків має стати обов’язкова сертифікація ШІ-рішень для гарантування їх безпечності та відповідності етичним нормам.

3. Соціальні аспекти зниження ризиків. Освітні ініціативи відіграють важливу роль у мінімізації ризиків використання ШІ. Підвищення рівня цифрової грамотності населення дозволяє краще розуміти принципи роботи технологій та уникати потенційних загроз. Викладання основ етичного використання ШІ у навчальних закладах сприятиме формуванню відповідального підходу до взаємодії з цими технологіями. Проведення

просвітницьких кампаній допоможе інформувати громадськість про потенційні ризики та можливості ШІ.

Контроль за впливом ШІ на ринок праці також є важливим аспектом. Автоматизація може призвести до втрати робочих місць у низці галузей, тому необхідно впроваджувати програми перекваліфікації для працівників, чиї професії перебувають під загрозою. Державна політика має регулювати вплив автоматизації на зайнятість та соціальні гарантії. Важливою є концепція «справедливого переходу», яка передбачає підтримку працівників, що постраждали від змін у структурі ринку праці.

Довіра та прийняття ШІ суспільством залежать від прозорості його використання. Впровадження механізмів громадського контролю дозволить забезпечити об’єктивний нагляд за розвитком технологій. Створення незалежних комісій для оцінки впливу ШІ на суспільство сприятиме відкритому обговоренню та врахуванню інтересів різних груп населення. Крім того, підтримка ініціатив із розробки етичних рекомендацій щодо взаємодії людини з ШІ допоможе встановити відповідні морально-етичні стандарти використання технологій.

Використання штучного інтелекту у сфері аналізу геополітичних ризиків стає важливим інструментом для адаптації стратегій безпеки. Запровадження автоматизованих систем моніторингу дозволяє ідентифікувати потенційні загрози на ранньому етапі, що підвищує ефективність запобіжних заходів. Крім того, міжнародна співпраця у сфері ризик-менеджменту сприяє обміну передовими практиками, що дозволяє підприємствам і державним структурам підвищувати рівень безпеки. Використання новітніх технологій забезпечує покращення захисту даних та мінімізацію кіберзагроз, що є критично важливим для інформаційної безпеки. На рис.3.1. представлена матриця TOWS-аналізу яка допоможе краще оцінити стратегії зниження ризиків використання ШІ.

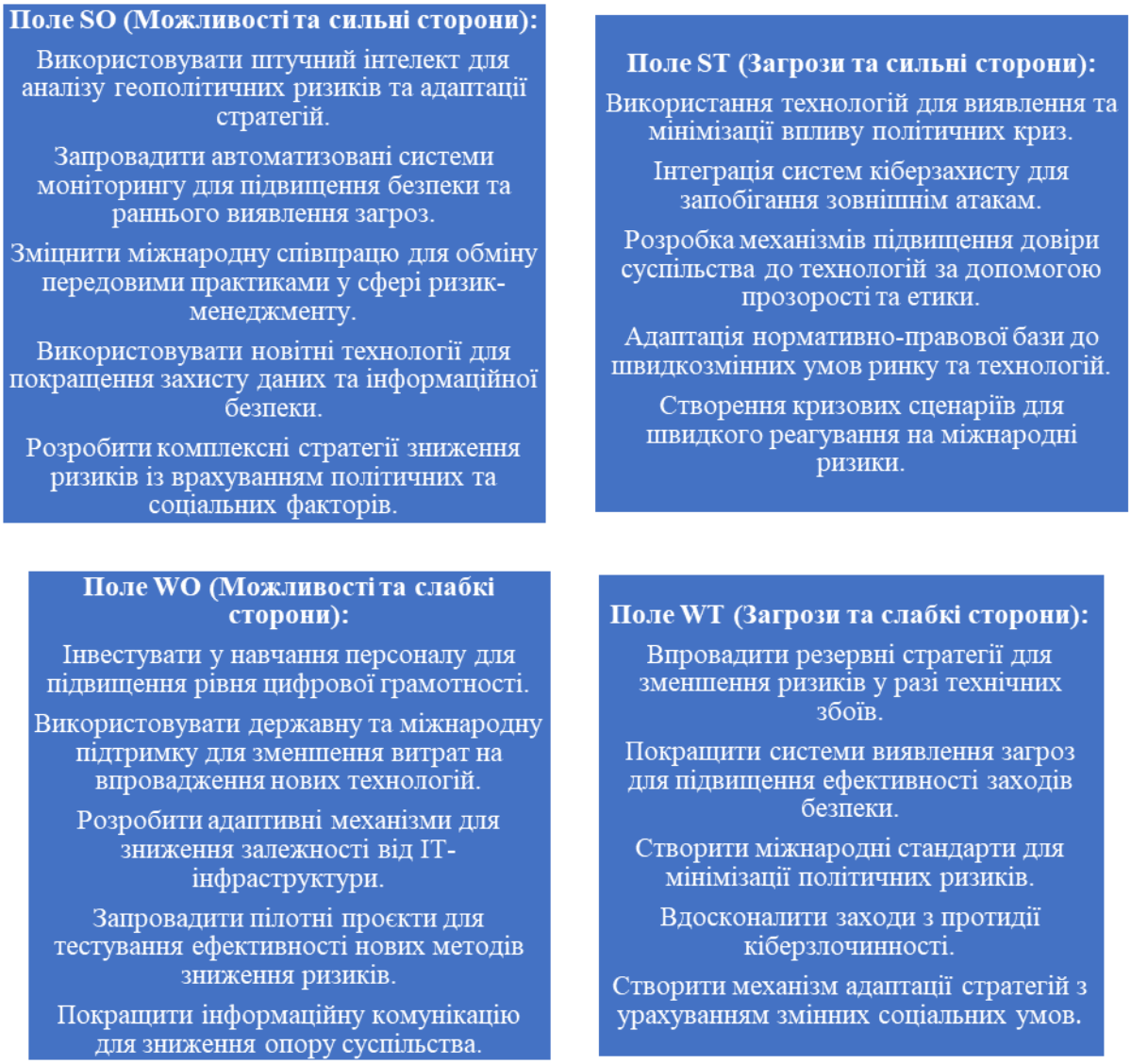


Рисунок 3.1.Матриця TOWS

*Джерело: створено автором на основі власних узагальнень*

- Використання сильних сторін для подолання загроз (ST-стратегії).

Інноваційні технології відіграють ключову роль у виявленні та мінімізації впливу політичних криз. Застосування сучасних систем кіберзахисту дає змогу ефективно протидіяти зовнішнім атакам, запобігаючи можливим витокам даних та маніпуляціям інформацією. Розробка механізмів підвищення довіри суспільства до технологій через прозорість та етичність їх використання є важливим аспектом стратегії. Адаптація нормативно-правової бази до змінних ринкових і технологічних умов дозволяє забезпечити більш ефективне регулювання ризиків. Крім того, створення

кризових сценаріїв забезпечує швидке реагування на міжнародні виклики та загрози, що дозволяє зменшити можливі наслідки кризових ситуацій.

- Подолання слабких сторін шляхом використання можливостей (WO-стратегії).

Один із ключових напрямів зниження ризиків – інвестування у навчання персоналу з метою підвищення рівня цифрової грамотності. Це сприяє ефективнішому використанню технологій та зменшенню ймовірності помилок при їх впровадженні. Державна та міжнародна підтримка може знизити витрати на інтеграцію нових технологій, що особливо важливо для компаній із обмеженим бюджетом. Для уникнення залежності від IT-інфраструктури необхідно розробляти адаптивні механізми, що дозволять компаніям швидко реагувати на технічні збої. Запровадження пілотних проєктів дає можливість оцінити ефективність методів зниження ризиків перед їх масштабним впровадженням. Також покращення інформаційної комунікації знижує опір суспільства щодо новітніх технологій, сприяючи їх швидшій адаптації.

- Зниження ризиків у разі слабких сторін та загроз (WT-стратегії).

Для ефективного зниження ризиків необхідно впроваджувати резервні стратегії, що дозволять мінімізувати негативні наслідки технічних збоїв. Покращення систем виявлення загроз сприятиме більш оперативному реагуванню на можливі ризики. Крім того, розробка міжнародних стандартів допоможе мінімізувати політичні ризики та забезпечити стабільність регулювання технологічних процесів. Вдосконалення заходів із протидії кіберзлочинності дозволить знизити вразливість систем до атак. Створення механізмів адаптації стратегій до змінних соціальних умов є важливим фактором для підтримання довгострокової стійкості бізнесу та державних структур до викликів сучасного світу.

В свою чергу на рис. 3.2. наведений розроблений нами механізм інтеграції штучного інтелекту у систему міжнародних відносин для зниження ризиків

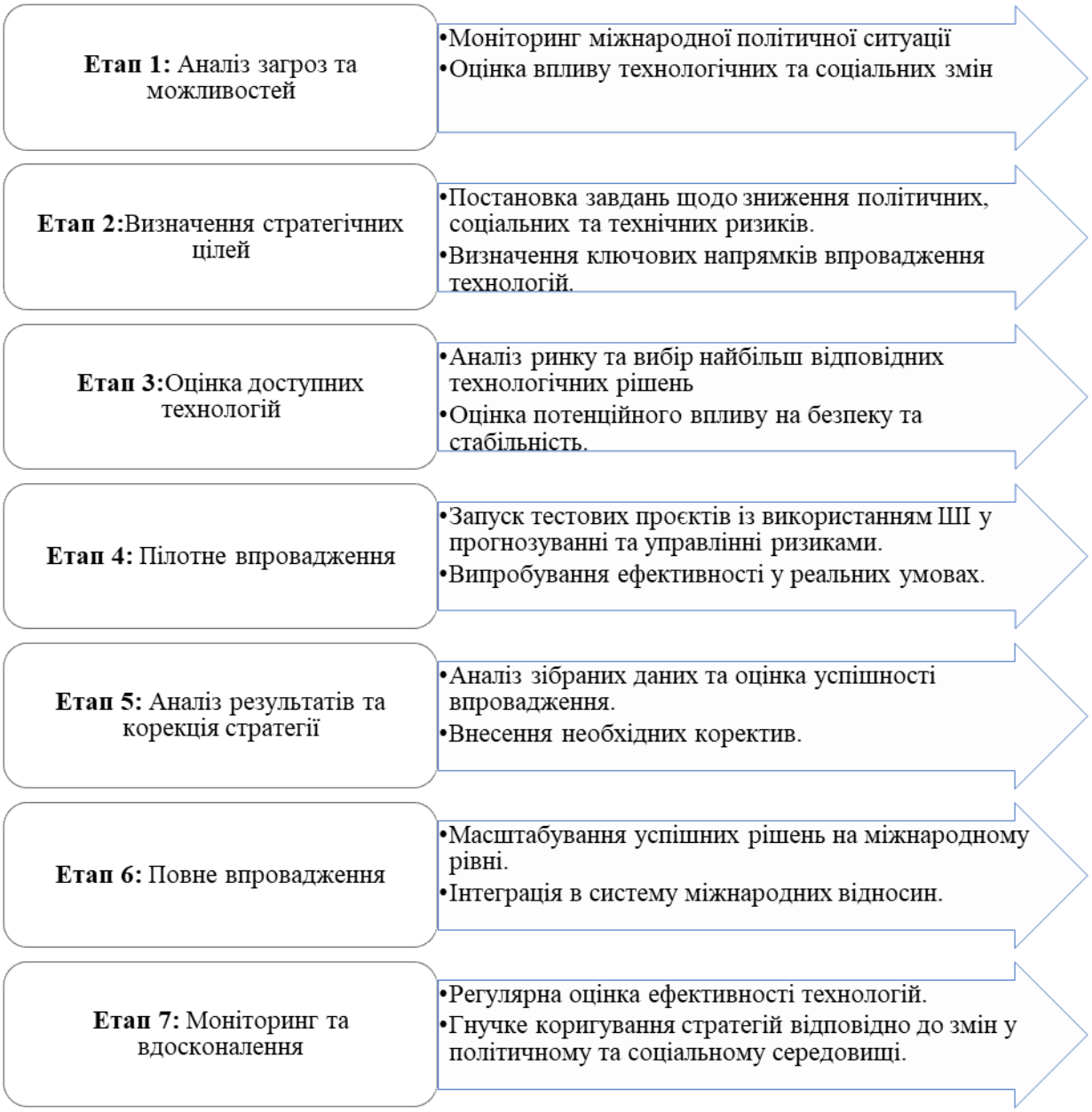


Рисунок 3.2. Механізм інтеграції штучного інтелекту у систему міжнародних відносин для зниження ризиків

*Джерело: створено автором на основі власних узагальнень*

На нашу думку, такий підхід дозволяє системно інтегрувати штучний інтелект у міжнародні відносини та ефективно знижувати ризики в умовах глобальної нестабільності.

Інтеграція штучного інтелекту та новітніх технологій у систему управління ризиками дозволяє значно підвищити ефективність управлінських процесів. Використання TOWS-аналізу забезпечує комплексний підхід до розробки стратегій зниження ризиків, що охоплює технічні, політичні та

соціальні аспекти. Завдяки цьому компанії та державні органи можуть швидко адаптуватися до нових викликів, покращувати захист інформації та знижувати рівень невизначеності в умовах динамічного середовища. Впровадження продуманих стратегій та механізмів управління ризиками сприяє довгостроковій стабільності та конкурентоспроможності на міжнародному ринку.

Отже, як ми бачимо комплексний підхід до зниження ризиків використання ШІ повинен включати технологічні, політичні та соціальні аспекти. Поєднання передових технічних рішень із міжнародним регулюванням і громадським контролем дозволить мінімізувати потенційні загрози та забезпечити безпечний розвиток ШІ у сучасному суспільстві. Для ефективної реалізації цих стратегій необхідна тісна співпраця між урядами, науковими установами, приватним сектором та громадянським суспільством. Лише завдяки спільним зусиллям можна забезпечити відповідальне використання ШІ на благо людства.

# ВИСНОВКИ

Штучний інтелект є однією з найбільш значущих технологій сучасності, яка активно впливає на різні сфери суспільного життя, включаючи міжнародні відносини, безпеку, економіку та правову сферу. Враховуючи його стрімкий розвиток, виникає необхідність у дослідженні його впливу на глобальні процеси, оцінці потенційних ризиків та розробці механізмів регулювання. У цій роботі було розглянуто ключові аспекти застосування ШІ та запропоновано стратегії мінімізації можливих загроз.

1. Дослідження концепції штучного інтелекту, його принципів функціонування та можливостей - тучний інтелект базується на методах машинного навчання, глибокого навчання, нейронних мереж і алгоритмах обробки інформації. Незважаючи на високий рівень розвитку, сучасні системи ШІ ще далекі від самостійного мислення та потребують ретельного регулювання. У майбутньому технологія матиме ще ширше застосування, зокрема у стратегічному плануванні та дипломатії.

2. Роль ШІ у трансформації міжнародного середовища - ШІ змінює підходи до управління, прогнозування криз і оптимізації міжнародних процесів. Він є важливим інструментом аналізу даних, що дозволяє більш ефективно реагувати на виклики міжнародної політики та безпеки. Однак його використання також створює нові ризики, які потребують глобального регулювання.

3. Безпекові аспекти впливу ШІ у глобальному контексті - ШІ активно застосовується у військовій сфері, системах національної безпеки та розвідки, що створює ризики щодо його автономності, можливих помилок і відсутності людського контролю. Використання автономних бойових систем потребує міжнародного регулювання для запобігання потенційним загрозам.

4. Основні загрози кібербезпеці, пов’язані із застосуванням ШІ - ШІ відіграє значну роль у забезпеченні кібербезпеки, автоматизуючи процеси

захисту, аналізу загроз і реагування на атаки. Водночас він може бути використаний зловмисниками для створення нових загроз, таких як автоматизовані кібератаки, маніпуляції даними та шахрайство. Тому необхідно вдосконалювати правове регулювання, підготовку фахівців і засоби контролю безпеки ШІ.

5. Ризики використання автономних бойових систем - автономні військові технології, зокрема безпілотники та роботизовані бойові системи, відкривають нові можливості, але водночас створюють загрози. Основними ризиками є відсутність людського контролю, можливі помилки в ідентифікації цілей та загроза дестабілізації глобальної безпеки. Запобігання неконтрольованому використанню таких систем потребує міжнародного контролю та етичних стандартів.

6. Етичні дилеми впровадження ШІ у сфері безпеки - використання ШІ у системах безпеки породжує питання конфіденційності, прозорості алгоритмів, соціальної відповідальності та прав людини. Надмірне використання ШІ може призвести до масового стеження, дискримінації та зниження довіри до державних інституцій. Для уникнення таких ризиків необхідні чіткі правові механізми та міжнародне регулювання.

7. Міжнародні механізми регулювання розвитку ШІ - міжнародне регулювання штучного інтелекту перебуває у стадії активного формування. Важливими ініціативами є Хіросімський процес, законодавчі акти ЄС, політика НАТО та зусилля ООН щодо встановлення глобальних стандартів. Головними викликами залишаються забезпечення прозорості технологій, моніторинг ризиків та впровадження ефективних механізмів контролю.

8. Роль міжнародної співпраці у забезпеченні безпечного використання ШІ - міжнародна співпраця є ключовим фактором у створенні безпечного середовища для розвитку ШІ. Угода між Україною та Великою Британією, ініціативи ЄС та НАТО сприяють прозорому регулюванню й обмеженню потенційних загроз. Баланс між безпекою та інноваціями дозволяє уникнути

зловживань технологією та забезпечує захист прав людини у цифровому просторі.

9. Розроблення стратегії мінімізації ризиків у технічному, політичному та соціальному аспектах – комплексний підхід до регулювання ШІ включає технічні вдосконалення (пояснювані алгоритми, підвищення кібербезпеки, захист даних), політичні ініціативи (міжнародне регулювання, сертифікація технологій, державні програми підтримки), а також соціальні заходи (підвищення цифрової грамотності, адаптація ринку праці, громадський контроль). Спільні зусилля держав, бізнесу та суспільства дозволять мінімізувати ризики та забезпечити безпечний розвиток ШІ.

Таким чином, розвиток штучного інтелекту супроводжується як значними можливостями, так і серйозними викликами. Впровадження ШІ в економіку, безпеку, військову справу та соціальні процеси потребує ретельного контролю, міжнародного регулювання та відповідального використання. Глобальна співпраця у сфері безпеки, кіберзахисту та правового регулювання є ключовим фактором у забезпеченні стабільного розвитку ШІ. Враховуючи стрімку динаміку технологічних змін, лише спільні зусилля держав, бізнесу, наукової спільноти та громадянського суспільства можуть гарантувати ефективне та безпечне застосування штучного інтелекту на благо людства.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційний сайт ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ». URL: https://metinvest.digital/ua (дата звернення: 20.02.2025)

2. Від Ш до І: що таке штучний інтелект та як він трансформує світ. URL: https://speka.media/ai/ (дата звернення: 20.02.2025)

3. Як діє штучний інтелект і перспективи його використання. Матеріали конференції «AI conference». URL: https://aiconference.com.ua (дата звернення: 20.02.2025)

4. Офіційний сайт ПП «ЛАНТЕК». URL: https://ula.lantec.ua(дата звернення: 20.02.2025)

5. Що таке штучний інтелект: історія, види та складові. URL: https://gigacloud.ua/articles/shho-take-shtuchnyj-intelekt-istoriya-vydy-ta-skladovi/ (дата звернення 20.02.2025)

6. Groumpos P. A Critical Historic Overview of Artificial Intelligence: Issues, Challenges, Opportunities and Threats. Artificial Intelligence and Applications Vol. XX Iss. XX yyyy. 2023. URL: https://www.researchgate.net/publication/372590389_A_Critical_Historic_Overview_of_Artificial_Intelligence_Issues_ (дата звернення 20.04.2025)

7. McCulloch S., Pitts W. «A logical calculus of the ideas immanent in nervous activity». The Bulletin of Mathematical Biophysics 5(4):115-133. 1943.

8. Turing A. Computing Machinery and Intelligence, Mind. LIX(236): 433—460. 1950.

9. A proposal for the Dartmouth Summer Research Project on Artificial Intelligence. URL: http://wwwformal.stanford.edu/jmc/history/dartmouth/dartmouth.html (дата звернення 21.02.2025)

10. Kasparov versus Deep Blue. 1997. URL: https:// www.chessgames.com/perl/chessplayer?pid=29912(дата звернення 21.03.2025)

11. Naisbitt J. Megatrends: Ten New Directions Transforming Our Lives Hardcover. Warner Books, Inc. First Edition. 1982. 290 p.

12. Cellan-Jones R. Stephen Hawking warns artificial intelligence could end mankind. URL: https://www.bbc.com/news/technology-30290540 (дата звернення 22.02.2025)

13. Улянівський Т. Штучний інтелект – це продовження еволюції. ZBRUC. 2017. URL: https://zbruc.eu/node/71907 (дата звернення 22.07.2025)

14. Keynes J. «Economic Possibilities for our Grandchildren» (1930), in Essays in Persuasion (New York : Harcourt Brace, 1932), 358–373. URL: https://assets.aspeninstitute.org/content/uploads/files/content/upload/Intro_and_Section_I.pdf (дата звернення 22.02.2025)

15. Marwala T. Introduction to Artificial Intelligence, Game Theory, and Mechanism Design in Politics. pp. 1–10. August 2023

16. Ndzendze B., Marwala T. Artificial Intelligence and International Relations Theories. Springer Nature Singapore. 2023

17. Elkus A. The futility of (narrow) speculation about machines and jobs. Medium. URL: https://medium.com/@Aelkus/the-futility-of-narrow-speculation-about-machines-and-jobs-a116a0672659 (дата звернення 2.02.2025)

18. The Future Today Institute. 2018 tech trends report. Future Today Institute. URL: https://bootstrapping.dk/wp-content/uploads/2018/03/FTI-2018-TrendReport.pdf (дата звернення 22.02.2025)

19. Scott B., Heumann S., Lorenz P. Artificial intelligence and foreign policy. Stiftung Neue Verantwortung (SNV). URL: https://www.stiftung-nv.de/sites/default/files/ai_foreign_policy.pdf (дата звернення 22.09.2025)

20. Wright N. How artificial intelligence will reshape the global order. Foreign Affairs. URL: https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order (дата звернення 2.02.2025)

21. European Parliament. Artificial Intelligence diplomacy. Europarl.europa.eu. URL:

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf (дата звернення 22.03.2025).

22. Horowitz M., Mahoney C. Artificial intelligence and the military: technology is only half the battle. War on the Rocks. URL: https://warontherocks.com/2018/12/artificial-intelligence-and-the-military-technology-is-only-half-thebattle/ (дата звернення 12.02.2025).

23. Yantaç C. E. Artificial intelligence, society and democracy. Turkish Policy Quarterly. URL: http://turkishpolicy.com/article/1097/artificial-intelligence-society-and-democracy (дата звернення 25.02.2025).

24. Galeotti M. The age of AI diplomacy. The spectator. 2023. URL: https://www.spectator.co.uk/article/the-ageof-ai-diplomacy/ (дата звернення 23.02.2025).

25. Voelsen D., Stanzel V. Diplomacy and artificial intelligence. Stiftung Wissenschaft und Politik (SWP). URL: https://www.swp-berlin.org/en/publication/diplomacy-and-artificial-intelligence#hd-d22571e579 (дата звернення 23.02.2025)

26. Future of Life Institute. Asilomar AI principles. Asilomar Conference of beneficial AI. USA. 5-8 January 2017. URL: https://futureoflife.org/2017/08/11/ai-principles/ (дата звернення 23.07.2025)

27. Council of Europe. Technological convergence, artificial intelligence and human rights. Committee on Culture, Science, Education and Media. Mr Jean-Yves Le Deaut. France, SOC 10 April 2017. Doc. 14288. URL: https://pace.coe.int/en/files/23531/html (дата звернення 23.04.2025)

28. OECD. Recommendation of the Council on Artificial Intelligence OECD/LEGAL/0449. 2019. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (дата звернення 24.02.2025)

29. United Nations Educational, Scientific and Cultural Organization. Draft text of the recommendation of the ethics of Artificial Intelligence. Rev.2. 25

June 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000377897 (дата звернення 24.06.2025)

30. G20 AI Principles. G20 Ministerial meeting on trade and digital economy. Japan, Tsubuka. 8–9 June 2019. URL: https://www.g20-insights.org/related_literature/g20-japan-ai-principles/ (дата звернення 24.02.2025)

31. International Monetary Fund. IMF Executive Board supports new strategy for data and statistics in the digital age. Press Release. 2018. No. 18/99. URL: https://www.imf.org/en/News/Articles/2018/03/20/pr1899imf-executive-board-supports-new-strategy-fordata-and-statistics-in-the-digital-age (дата звернення 24.03.2025)

32. NATO. Summary of the NATO Artificial Intelligence Strategy. Belgium. Brussels. 22 October 2021. URL: https://www.nato.int/cps/uk/natohq/official_texts_187617.htm?selectedLocale=en (дата звернення 14.02.2025)

33. Stanley-Lockman Z., Trabucco L. NATO's role in responsible AI governance in military affairs. In: The Oxford Handbook of AI governance. Eds: by J. Bullock, Y.-Ch. Chen, J. Himmelreich, V. M. Hudson, A. Korinek, M. Young, Zhang, B. 2022

34. OECD.AI. Powered by EC/OECD (2021), database of national AI policies. 2021. URL: https://oecd.ai/en/dashboards/countries/EuropeanUnion (дата звернення 29.03.2025)

35. European Commission. Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence. Brussels. 8 April 2019. URL: https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelinestrustworthy-ai (дата звернення 25.02.2025)

36. European Commission. On Artificial Intelligence – A European approach to excellence and trust. White Paper. COM(2020) 65 final. Brussels. 19 February 2020. URL: https://ec.europa.eu/info/sites/default/files/commissionwhite-paper-artificial-intelligence-feb2020_en.pdf (дата звернення 25.05.2025)

37. African Union. The digital transformation strategy for Africa (2020-2030). Ethiopia, Addis Ababa. 2019. URL: https://au.int/sites/default/files/documents/38507- doc-dts-english.pdf (дата звернення 25.08.2025)

38. State Council. Guiding opinions of the State Council on actively propelling the Internet plus Action Plan. Lexis China. 1 July 2015 no. 40. URL: https://hk.lexiscn.com/law/guiding-opinions-of-the-state-council-on-activelypropelling-the-internet-plus-action-plan.html (дата звернення 25.02.2025)

39. Застосування ШІ у кібербезпеці: роль та переваги. URL: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi (дата звернення 26.02.2025)

40. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ (дата звернення 26.02.2025)

41. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks (дата звернення 16.02.2025)

42. Корпоративна кібербезпека: Роль ШІ у захисті даних. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection (дата звернення 6.02.2025)

43. Global AI in Military Market By Component. URL: https://market.us/report/artificial-intelligence-inmilitary-market/

44. REAIM 2023 Call to Action. URL: https://www.government.nl/ministries/ministry-of-foreignaffairs/documents/publications/2023/02/16/reaim-2023-call-to-action (дата звернення 26.03.2025)

45. Science & Technology Trends 2020-2040. Exploring the S&T Edge. NATO Science & Technology Organization. (n. d.). 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 (дата звернення 26.02.2025)

46. The Top 10 AI Applications for Military Use. URL: https://www.linkedin.com/pulse/top-10-aiapplications-military-use-markets-us-icjgf/ (дата звернення 26. 06.2025)

47. Artificial Intelligence for Military Logistics – Current Applications. URL:https://emerj.com/ai-sectoroverviews/artificial-intelligence-military-logistics/ (дата звернення 26.02.2025)

48. Трофименко, О. Г., Яремчук, М. В. Штучний інтелект у військовій сфері. Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика: матер. міжнар. наук.- практ. конф., 2023, 144–148

49. Shopsin, J. (n. d.). What is Artificial Intelligence in CCTV? URL:https://www.securitycameraking.com/securityinfo/what-is-artificial-intelligence-in-cctv/ (дата звернення 16.02.2025)

50. AI-Powered Cybersecurity: Top Use Cases in 2023. URL: https://hackernoon.com/ai-poweredcybersecurity-top-use-cases-in-2023 (дата звернення 26.02.2025)

51. Трофименко, О. Г., Кіх, Я. Т. Застосування алгоритмів штучного інтелекту для військових задач. Сучасні технології в енергетиці, електромеханіці, системах управління та машинобудуванні: матер. VI всеукр. наук.-практ. інтернет-конференції., 2023

52. AI copilot enhances human precision for safer aviation. MIT News. URL: https://news.mit.edu/2023/aico-pilot-enhances-human-precision-safer-aviation-1003 (дата звернення 18.02.2025)

53. Як штучний інтелект допомагає Україні боротися з ворогом. URL: https://info.nic.ua/uk/bloguk/artificial-intelligence-2/ (дата звернення 26.02.2025)

54. Donham, B. P. (n. d.). Data Desert: Military Medicine's Artificial Intelligence Implementation Barriers. URL: https://military-medicine.com/article/4256-data-desert-military-medicine-s-artificial-intelligenceimplementation-barriers.htm (дата звернення 26.02.2025)

55. BAE Systems awarded contract to produce warfare systems for the F-15 Eagle. URL: https://www.aeroflap.com.br/en/bae-systems-recebe-contrato-para-producao-de-sistemas-de-guerra-parao-f-15-eagle/ (дата звернення 26.02.2025)

56. What is Reinforcement Learning? URL: https://aws.amazon.com/what-is/reinforcement-learning/ (дата звернення 09.02.2025)

57. Truby J. Governing artificial intelligence to benefit the UN sustainable development goals. Sustainable Development, 28(4), 946 – 959

58. Times Now Bureau, ―Delhi Metro Magenta Line driverless train rams into wall, DMRC Says accident due to ‗Human Error', 2017

59. Russell S. J. and Norvig P. Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited,, 2016

60. Goffi E. R. Teaching Ethics Applied to AI from a Cultural Standpoint: What African "AI Ethics" for Africa? In AI Ethics in Higher Education: Insights from Africa and Beyond (pp. 13 -26). Cham: Springer International Publishing.

61. Kiemde, S. M. A., & Kora, A. D. Towards an ethics of AI in Africa: rule of education. AI and Ethics, 1 – 6. 2022

62. Світова битва за ШІ-регулювання. URL: https://forbes.ua/innovations/svitova-bitva-za-kontrol-shi-chiy-tabir-kontrolyu-za-shi-peremozhe-pomirkovaniy-chi-suvoriy-rozsliduvannya-politico-26032024-20143 (дата звернення: 02.03.2025)

63. Міжнародні стандарти регулювання штучного інтелекту. URL: https://www.crowe.com/ua/croweacu/news/international-standards-for-regulating-artificial-intelligence (дата звернення: 02.03.2025)