МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ВОЄННА АКАДЕМІЯ ІМЕНІ ЄВГЕНІЯ БЕРЕЗНЯКА

Алексєєнко І.В., Дзядук Д.О., Кармазіна М.С.,
Лисецький Ю.М., Мокляк С.П., Смолянюк В.Ф., Ткач І.М.

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Монографія

Київ 2025

УДК 004.8:351.86
М74

Рекомендовано до друку Вченою радою
Воєнної академії імені Євгенія Березняка
(протокол № 4 від 30 квітня 2025 року)

Автори:
Алексєєнко І.В. — доктор політичних наук, професор;
Дзядук Д.О. — доктор філософії, старший дослідник;
Кармазіна М.С. — доктор політичних наук, професор;
Лисецький Ю.М. — доктор технічних наук, доцент;
Мокляк С.П. — доктор політичних наук, професор;
Смолянюк В.Ф. — доктор політичних наук, професор;
Ткач І.М. — доктор економічних наук, професор.

Рецензенти:
Бегма В.М — доктор економічних наук, професор, головний науковий співробітник відділу воєнної та воєнно-економічної політики Національного інституту стратегічних досліджень;

Петров В.В. — доктор політичних наук, доцент, професор кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка.

За загальною редакцією: С.П. Мокляка

М74 **Штучний інтелект як чинник забезпечення національної безпеки** : монографія / Алексєєнко І.В., Дзядук Д.О., Кармазіна М.С., Лисецький Ю.М., Мокляк С.П., Смолянюк В.Ф., Ткач І.М.; за заг. ред. С.П. Мокляка. — Київ : Видавець Бихун В.Ю., 2025. 228 с.

ISBN 978-617-7699-86-5

Зміна ландшафту війни і безпеки суттєво вплинула на різні елементи оборони. Помітні тренди, такі, як технологічний прогрес, зростання ролі недержавних акторів і зміна геополітичної динаміки, трансформують спроможності і стратегії держав. Штучний інтелект змінює різні оборонні спроможності, зокрема логістику, командування і управління та розвідувальний аналіз. Перегони щодо інтеграції штучного інтелекту в оборонні стратегії продовжують прискорюватися, що зумовлено стратегічними перевагами, які вони пропонують. Провідні країни, зокрема США, Китай інвестують чималі кошти в дослідження і розробки штучного інтелекту, щоб отримати конкурентну перевагу. Розробка систем озброєнь, засобів кіберзахисту та розвідувальних платформ, керованих штучним інтелектом, підкреслює глобальний акцент на використанні цих технологій для досягнення військової переваги. Монографія розрахована на науковців, викладачів, аспірантів та широке коло читачів.

ISBN 978-617-7699-86-5

ЗМІСТ

ПЕРЕДМОВА

Стратегія воюючої держави нерозривно пов'язана з оцінкою наявного потенціалу — людського й матеріального та практичним застосуванням сил та засобів, необхідних для досягнення поставленої мети.

Історія людства знає чимало прикладів, коли несприйняття наукових та технологічних досягнень або несвоєчасна реакція на них призводили до далекосяжних наслідків, дуже часто при цьому не тільки до невпізнанності трансформуючи основні принципи збройної боротьби, а й кардинально перетворюючи існуючий воєнно-політичний світо устрій, змінюючи хід всього історичного процесу[1].

В оборонних галузях провідних країн світу сьогодні вже чітко окреслилася тенденція розвитку на основі принципів та функціональних якостей Четвертої промислової революції, мультиплікаторних зразків, комплексів та систем озброєння та військової техніки (ОВТ), які за своїми можливостями у рази переважають або потенційно переважатимуть наявне озброєння. Такі зразки, комплекси, системи ОВТ за своїми бойовими характеристиками та наслідками від застосування будуть зіставні із високоточною й навіть з ядерною зброєю. Відповідно до цього змінюються погляди на зміст, тактику і стратегію збройної боротьби – вони розглядаються вже не як зіткнення бойових одиниць, що вражають одна одну в ході вогневого протиборства та захоплення території супротивника, а як зіткнення багатофункціональних бойових систем, основною метою якого є позбавлення конфронтуючої системи здатності до дії.

Нові тренди суттєво впливають на різні елементи та складові оборони, що потребує від військових організацій адаптації своїх стратегій і посилення спроможностей для ефективного вирішення складних завдань сучасної війни.

Використання технологій штучного інтелекту (ШІ) у нових системах управління озброєнням дасть можливість здійснити прорив під час ведення бойових дій. Такі системи дозволять прискорити прийняття рішень з урахуванням максимальної кількості чинників та значно скоротити цикл управління військами (силами), а також підвищити їхні бойові можливості. У цей час найбільших результатів американські фахівці досягли в галузі "глибокого

[1] Горбулін В. Забезпечення воєнної безпеки держави шляхом розвитку воєнно-технологічної сфери // Центр дослідження армії, конверсії та роззброєння. – 2021, 24 листопада. — URL: https://tinyurl.com/43hjuv3y

машинного навчання". Це стало можливим завдяки швидкому прогресу в розвитку багаторівневих штучних нейронних мереж. Технології розпізнавання образів та машинне навчання, які використовуються в сучасному ШІ, можуть забезпечити високий ступінь автоматизації прийняття управлінських рішень під час аналізу та обробки інформації від різних джерел.

У Стратегії розвитку штучного інтелекту Міністерства оборони США стверджується, що штучний інтелект покращить процес прийняття рішень і оперативну ефективність, підкреслюючи його стратегічну важливість у майбутніх військових операціях. Інтеграція технологій ШІ все частіше розглядається як мультиплікатор сили.

Оборонна промисловість також переживає зміни в управлінні закупівлями і ланцюжками постачання через попит на швидкі інновації. Закон США "Про національну оборону" наголошує на необхідності "гнучкості процесів закупівель, щоб йти в ногу з технологічним прогресом", вказуючи на те, що традиційні методи закупівель можуть перешкоджати своєчасному придбанню нових технологій. Це потребує більш адаптивного підходу до закупівель в оборонному секторі.

Крім того, на характер війни все більше впливають гібридні загрози, які поєднують звичайні та нерегулярні тактики. У Декларації Варшавського саміту НАТО вказано наступне: "Ми стоїмо перед складним середовищем безпеки, яке характеризується гібридними загрозами", що підкреслює необхідність адаптації оборонних секторів до широкого спектру викликів, зокрема кампаній з дезінформації та нетрадиційних тактик+ ведення війни.

ЧАСТИНА І
СТРАТАГЕМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

РОЗДІЛ 1
НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ: ВИТОКИ ТА ПРІОРИТЕТИ СЬОГОДЕННЯ (2014—2025 РОКИ)

Володимир СМОЛЯНЮК,
доктор політичних наук, професор

Необхідна передмова. Базис національної безпеки України у вигляді чітко сформованої теоретичної платформи у засадничих державотворчих документах — Декларації про державний суверенітет України від 16.07.1990 р. [1] та Акті проголошення незалежності України від 24.08.1991 р. [2] — був відсутнім. У Декларації йшлося про "українську націю", "національну державу", "національну державність", "всі національності", "національно-культурний розвиток", "національно-культурне відродження", "національно-етнографічні особливості", "національно-культурні потреби", "національні цінності", проте не згадувалося про національну безпеку. В Акті проголошення незалежності про неї також не йшлося.

Дався взнаки негативний радянський спадок: у попередній державі в її партійно-ідеологічній, законодавчій, державно-управлінській, воєнно-політичній, науково-освітній та інших сферах термін *національна безпека* (як і "радянська нація") не вживався. Замінниками залежно від конкретної ситуації виступали державна безпека, міжнародна безпека, воєнна (оборонна) безпека, екологічна безпек". Як наслідок, рання державотворча риторика України на зламі 1990–1991 рр. терміну "національна безпека" не містила. Окремі науковці у 90-х роках взагалі пропонували відмовитися від нього, апелюючи, що англійському прикметнику national більше відповідав український аналог державний [3]. Відтак імплементація словосполучення національна безпека в українські нормативно-правові регулятори та державотворчі реалії відбувалася із помітним запізненням.

Кроком уперед в осмисленні національної безпеки стала Постанова Верховної Ради України від 02.07.1993 р. "Про Основні напрями зовнішньої політики України". У документі йшлося про "стратегічні та геополітичні інтереси, пов'язані з забезпеченням національної безпеки України та захистом її політичної незалежності" [4]. Розкриття безпекової проблематики у

документі відбувалося шляхом застосування низки взаємопов'язаних (при цьому еклектичних) термінів: "загроза національній безпеці", "система міжнародної регіональної безпеки", "загальноєвропейська безпека", "забезпечення загальної і регіональної безпеки", "забезпечення міжнародного миру і безпеки", "універсальна безпека". Однією з головних пріоритетних функцій зовнішньої політики України відповідно до її найважливіших загальнонаціональних інтересів та завдань було визначено "забезпечення національної безпеки". Постанова (яка ґрунтувалась на ідеалізованому політичному мисленні початку 90-х років) указувала на шляхи виконання цієї функції, до яких були віднесені створення всеохоплюючих безпекових систем, ядерне роззброєння держав, нерозповсюдження технологій виготовлення та застосування інших видів зброї масового знищення тощо.

У Конституції України від 28.06.1996 р. термін національна безпека згадується в кількох контекстах [5]. Відповідно до ст. 92, виключно законами України визначаються "основи національної безпеки". Відповідно до ст. 106, Президент "забезпечує національну безпеку" та "очолює Раду національної безпеки і оборони". Відповідно до ст. 107, "Рада національної безпеки і оборони є координаційним органом з питань національної безпеки і оборони України при Президентові України". Відповідно до ст. 116, Кабінет Міністрів "здійснює заходи щодо забезпечення обороноздатності і національної безпеки України". Конституційний рівень рефлексії діяльності з питань національної безпеки України засвідчив безпосередню причетність легітимних гілок влади до цієї надважливої сфери державно-політичної діяльності.

Постанова Верховної Ради України від 16.01.1997 р. "Про Концепцію (основи державної політики) національної безпеки України" вперше визначила суб'єкт-об'єктну структуру національної безпеки, принципи її забезпечення, національні інтереси України, загрози національній безпеці (в політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній сферах), основні напрямки політики національної безпеки в зазначених сферах [6]. Власне національна безпека України у документі визначалась як "стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз" та необхідній умові "збереження та примноження духовних і матеріальних цінностей". Отже, національну безпеку України, починаючи з 1997 р., пропонувалося розуміти як стан захищеності інтересів.

Критично слід зауважити, що переліку "життєво важливих інтересів особи, суспільства та держави" ні у цитованій Постанові, ні в наступних документах з питань національної безпеки не пропонувалось. На практиці для осіб, причетних до забезпечення національної безпеки, завдання визначались більш спрощеним підходом: національна безпека — це стан захищеності національних інтересів. Останні у вигляді пріоритетних національних інтересів, пріоритетів національних інтересів, життєво важливих національних інтересів, фундаментальних національних інтересів присутні в національному законодавстві, починаючи з 90-х років.

Наступним документом у царині національної безпеки став Закон України від 05.03.1998 р. "Про Раду національної безпеки і оборони України" [7]. Головою Ради є Президент України, який формує персональний склад цього конституційного органу та головує на його засіданнях. До складу Ради за посадою входять Прем'єр-міністр України, Міністр оборони України, Голова Служби безпеки України, Міністр внутрішніх справ України, Міністр закордонних справ України. Структура постійних членів Ради виявилась виправданою в умовах перманентного накопичення воєнних та інших загроз як довкола України, так і у внутрішньому суспільно-політичному просторі.

Етапною нормативно-правовою віхою у сфері національної безпеки і оборони України став Закон України від 19.06.2003 р. "Про основи національної безпеки України" [8]. Інноваціями даного Закону стали: розширення кола суб'єктів забезпечення національної безпеки; визначення пріоритетів національних інтересів України; визначення загроз національним інтересам і національній безпеці України у дванадцяти важливих сферах — зовнішньополітичній, державної безпеки, воєнній та сфері безпеки державного кордону, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, цивільного захисту, екологічній, інформаційній; визначення основних напрямів державної політики національної безпеки України у названих вище сферах; визначення повноважень та основних функцій суб'єктів забезпечення національної безпеки — Президента України, Верховної Ради України, Ради національної безпеки і оборони України, Кабінету Міністрів України, Національного банку України, міністерств та інших центральних органів виконавчої влади, Служби безпеки України, Служби зовнішньої розвідки України, місцевих державних адміністрацій та органів місцевого самоврядування, Воєнної організації держави, органів і підрозділів цивільного захисту, правоохоронних органів, судів загальної юрисдикції, прокуратури України, громадян України; визначення суб'єктів контролю за здійсненням заходів щодо забезпечення національної безпеки.

Вадами цього законодавчого акту стали такі: замовчування кількох сфер забезпечення національної безпеки — енергетичної, фінансової, демографічної, міграційної, етнонаціональних відносин, міжконфесійних відносин, морської; уникнення необхідності формулювання загроз у надважливих для України енергетичній та фінансовій сферах, серед яких домінантною загрозою було засилля російського капіталу та олігархічні зловживання; інерційне (пострадянське) визнання Воєнної організації держави одним з основних суб'єктів забезпечення національної безпеки.

Про Воєнну організацію держави (ВОД) йшлося в Законах України "Про основи національної безпеки України" (згаданому вище) та "Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави" [9]. У першому з цих законів ВОД визначається як "сукупність органів державної влади, військових формувань, утворених відповідно до законів України, діяльність яких перебуває під демократичним цивільним контролем з боку суспільства і безпосередньо спрямована на

захист національних інтересів України від зовнішніх та внутрішніх загроз". Другий закон альтернативно визначає ВОД як охоплену єдиним керівництвом "сукупність органів державної влади, військових формувань, утворених відповідно до Конституції і законів України, діяльність яких перебуває під демократичним контролем суспільства і відповідно до Конституції та законів України безпосередньо спрямована на вирішення завдань захисту інтересів держави від зовнішніх та внутрішніх загроз". Два закони, прийняті в один день, по-різному розкривали спрямованість діяльності ВОД — "захист національних інтересів" та "захист інтересів держави". Роком пізніше термін "ВОД" було повторено в Законі України від 18.11.2004 р. "Про організацію оборонного планування" [10].

Отже, в України більше двох десятиріч існувала низка силових структур, які на різних підставах могли бути визначені як складники ВОД. Ними були: за прямою вказівкою в законодавстві — Збройні Сили України, Служба зовнішньої розвідки України, війська Цивільної оборони України; за функцією захисту держави шляхом безпосереднього ведення бойових дій — Збройні Сили України, внутрішні війська МВС України, Державна спеціальна служба транспорту Міністерства транспорту і зв'язку України, Державна прикордонна служба України; за ознакою комплектування військовиками, які мають військові звання, проходять військову службу та на яких поширюється соціальний і правовий захист, умови пенсійного забезпечення, передбачені для військовиків — Збройні Сили України, внутрішні війська МВС України, Державна прикордонна служба України, СБУ, Служба зовнішньої розвідки України, Державна спеціальна служба транспорту, Управління державної охорони [11, с. 238]. Іншими словами, практично будь-яка комбінація законних збройних формувань Української держави могла бути віднесена до Воєнної організації, яка при цьому не керувалася з єдиного державного центру. Рада національної безпеки і оборони (РНБОУ), володіючи координаційними функціями, на роль управлінської інстанції не могла претендувати.

Як видно, тривалий час Україна декларувала необхідність створення та зміцнення ВОД, націленої на державну протидію загрозам зовнішнього та внутрішнього походження. На це були орієнтовані Збройні Сили (зовнішній аспект протидії), МВС, СБУ (внутрішній аспект протидії), інші силові структури. Таку ситуацію можна визначити як непродуману імплементацію у воєнно-політичні реалії XXI ст. ретроспективних підходів щодо збройного гарантування національних інтересів. Воєнна організація Української держави у 90-х роках формувалася та діяла як набір окремих силових структур, очільники яких переймались насамперед відомчими проблемами без врахування національних інтересів, необхідності дотримання державних підходів щодо реагування на загрози, а також залучення структур громадянського суспільства до вирішення безпекових і оборонних завдань.

В українській воєнній сфері тривалий час репродукувався старий (радянський) тип мислення. 1991 р. Україна не проголосила себе спадкоємницею українських державних утворень XX ст. та її військових формувань.

Політичним наслідком цього стало те, що держава не пішла шляхом формування національних збройних сил, як це зробили держави Балтії. Ігнорування мілітарної спадкоємності призвело до того, що радянська (проросійська) ментальність у 1990-х роках перейшла та закріпилась у ЗС України, а її носії почувалися доволі впевнено [12, с. 214].

Риторика України довкола ВОД як суб'єкта забезпечення національної безпеки контрастувала із зовнішньополітичними цілями, зокрема намірами вступу до НАТО. Країни Альянсу не використовують лексичну конструкцію "воєнна організація держави". 32 країни НАТО (станом на 2025 р.) — це 32 сумісних між собою секторів безпеки і оборони суверенних держав, якісні характеристики яких є принципово відмінними від воєнно-організаційних. Демократична держава навіть на підготовчому етапі вступу до Альянсу має оперувати терміном "сектор безпеки і оборони" як суб'єктом забезпечення національної безпеки, фіксуючи це на законодавчому рівні та відмовляючись від радянських штампів. Україна потрапила у власноруч зроблену пастку, проголосивши у 1998 р. наміри "повномасштабної інтеграції до європейських та євроатлантичних структур" [13], але використовуючи при цьому воєнно-політичний лексикон авторитарних (тоталітарних) систем XX ст.

У 90-і роки виник вододіл між пострадянськими державами на основі протилежного розуміння політичної суб'єктності у сфері забезпечення обороноздатності. ВОД у її пострадянському тлумаченні — це атрибут насамперед президентських політичних систем, які не лише охоче використовують радянський силовий спадок з метою політичного самозбереження, а й активно розвивають його в інтересах правлячих режимів. Воєнна організація була й залишається основним інструментом реалізації безпекової і воєнної політики у росії, Білорусі, Казахстані, центральноазійських республіках. Донедавна ним оперували у Вірменії.

На противагу цьому, сектор безпеки і оборони є атрибутом парламентських або змішаних політичних систем, що виникли на пострадянському просторі. Йдеться про Латвію, Литву, Естонію (членів НАТО), а також Молдову, Україну, Грузію (із застереженнями). Україна фактично створила прецедент проголошення євроатлантичної інтеграції як фундаментального національного інтересу XXI ст. на основі використання функціональних спроможностей Воєнної організації держави XX ст. Результати подібного схрещування виявились невтішними. В умовах мирного часу (до 2014 р.) Україна не розглядалася керівництвом Альянсу як "зрілий" кандидат на його поповнення. В умовах російсько-української війни перспектива членства України в Організації Північноатлантичного договору теж відсунута на невизначену перспективу.

Отже, Закон України "Про основи національної безпеки України" з позицій сьогодення слід оцінювати як "передвоєнний" нормативно-правовий акт, який попри свою змістовну важливість та закладений у нього державно-управлінський потенціал у безпековій сфері, не став основою зміцнення безпекової та оборонної сфер Української держави напередодні її воєнного

зіткнення з РФ. Проросійськими політичним силами, що діяли в Україні, відкидалась сама можливість російського вторгнення на українську територію. За їхньої активної участі Україна послідовно позбавлялась мілітарних можливостей, успадкованих від попередньої держави (роззброювалась), а й цілеспрямовано готувалась до вступу в контрольовані Москвою пострадянські структури (ОДКБ, Митний Союз, ЄврАзЕС, інші структури).

Російсько-український збройний конфлікт розпочався через 11 років після прийняття цього першого в історії незалежної України законодавчого акту з питань національної безпеки. Проте законодавчий орган двох наступних скликань (5-го та 6-го, що діяли відповідно у 2006—2007 та 2007—2012 роках), не визнав за необхідне його оновлення в умовах ескалації військових приготувань сусідньої держави. Така ж споглядальна позиція була властива парламенту 7-го скликання, який з жовтня 2012 р. по лютий 2014 р. не зміг виправити ситуацію в галузі національної безпеки.

Подальше нормативно-правове насичення сфери національної безпеки України відбувалося шляхом підготовки й публічного оприлюднення Стратегії національної безпеки України. Цей документ підписувався новим главою держави та виступав умовною декларацією намірів президентської команди, що здобула перемогу на виборах, у безпеково-оборонній сфері. Це стосується Стратегій національної безпеки України від 12.02.2007 р. [14], 08.06.2012 р. [15], 26.05.2015 р. [16], а також від 14.09.2020 р. [17]. Як видно, в Україні із запізненням (на 16-у році незалежності) було започатковано традицію стратегічного цілепокладання глави держави у сфері національної безпеки на сторінках окремого документу, який упродовж терміну його перебування на посаді мав бути регулятором поточної безпекової політики.

Слід вказати на надмірну декларативність Стратегій національної безпеки України 2007 та 2012 рр., які мало що змінили у практичній діяльності державних органів з питань убезпечення України. Стратегія 2015 р. як документ держави, поставленої перед необхідністю збройного захисту національних інтересів в умовах нав'язаної РФ війни, називав речі своїми іменами — окупація, воєнна агресія, безкарне застосування сили, російська загроза, бойові дії, квазідержавні утворення, незаконні збройні формування тощо. Стратегія 2020 р. знову виявилась надмірно насиченою загальними фразами. Крім того, замість відведеного законодавством терміну в 6 місяців вона була підписана на 16-му.

Маємо визнати, попри безсумнівний розвиток теорії національної безпеки у незалежній Україні в теоретично-концептуальному та організаційно-практичному аспектах, проявом чого стала розробка та прийняття (підписання) низки важливих документів націєбезпечної спрямованості, Українська держава виявилася безпорадною перед російськими загрозами, спрямованими на її знищення. Період 1991–2014 рр. може бути позначений як імітаційний у контексті становлення системи національної безпеки України. Держава пропустила момент трансформації російського імперства від його медійно-пропагандистського до практично-наступального вигляду. Реакція

України на ескалацію військових загроз з боку РФ мала відбутися на початку 2007 р., коли В.Путін у відомій мюнхенській промові відкрито заявив про небажання росії миритися з "нав'язаним" їй статусом маловпливового учасника світової політики та артикулював готовність Кремля до силового відновлення глобальних позицій, якими раніше володів СРСР [18].

Контрдії України, спрямовані проти російських мілітарних приготувань, були слабкими. Безрезультатними виявились «передвоєнні» парламентські слухання від 23.05.2012 р. "Про стан та перспективи розвитку Воєнної організації та сектору безпеки України". Слухання констатували критичні негаразди у сфері забезпечення національної безпеки і оборони України [19]: стан Збройних Сил України, як і оборонно-промислового комплексу, характеризується глибокою депресією; небезпечних масштабів набуває деградація військово-технічного потенціалу Збройних Сил; повільно здійснюється реформування діяльності правоохоронних органів у відповідності з європейськими стандартами, призначених забезпечувати національну безпеку; недостатньо враховується та обставина, що в українському суспільстві відбувається політична радикалізація, зростають екстремістські настрої, що може створювати реальну загрозу громадському спокою, державному суверенітету і територіальній цілісності України.

Перебування на посаді глави Української держави В. Януковича (з 25.02.2010 р. по 22.02.2014 р.) оцінюється як час прискореного демонтажу ЗС України як найбільш боєздатного складника тогочасної системи забезпечення національної безпеки. 2011—2014 рр. стали періодом цілеспрямованої, узгодженої з політичним керівництвом РФ, повної ліквідації бойового потенціалу українського війська, його доведення до стану, що виключав саму можливість силової реакції України на деструктивні зовнішні впливи. Про це свідчать призначення на посаду Міністра оборони України громадян РФ Дмитра Саламатіна (лютий-грудень 2012 р.) та Павла Лєбєдєва (грудень 2012 р. — лютий 2014 р.). Метою подібних кадрових призначень було унеможливлення силового спротиву України та створення необхідних умов входження України до 2015 р. до складу створених РФ Митного Союзу та Євразійського Економічного Простору [20, с. 117]. У випадку реалізації подібних планів на порядок денний з високою вірогідністю вийшло б питання входження України з її значними мілітарними (військово-промисловими) можливостями до Організації Договору про колективну безпеку.

Можемо підсумувати: державотворчі зусилля України мирного періоду розвитку (1991—2013 рр.) призвели до формування недосконалої статичної моделі забезпечення національної безпеки. Її складниками стали: національні інтереси та національні цінності України, оформлення яких на сторінках державних документів було надто абстрактним (контурним); суспільні сфери, де має зосереджуватися першочергова діяльність з питань забезпечення національної безпеки; очікувані деструктивні впливи на сферу національної безпеки (виклики, загрози, небезпеки, ризики), які в аналітичних документах комбінувалися довільно (ризик — виклик, небезпека — ризик,

загроза — небезпека та ін.); суб'єкт-об'єктна основа націєбезпечної діяльності. Серед суб'єктів забезпечення національної безпеки особливе місце було відведене РНБО України, а також сектору безпеки і оборони, який упродовж довоєнного періоду йменувався радянським термінологічним анахронізмом «Воєнна організації держави». Подібна вербальна недбалість ототожнювала Україну з президентськими пострадянськими державами (насамперед РФ) та повністю суперечила євроатлантичній стратегії держави.

Поступово запрацювала система законодавчого (нормативно-правового) забезпечення національної безпеки України, що засвідчили Закон України від 19.06.2003 р. "Про основи національної безпеки України" та Стратегії національної безпеки України від 12.02.2007 р. та 08.06.2012 р., підписані тогочасними Президентами України. Проте статична модель забезпечення національної безпеки виконувала насамперед імітаційну роль, створюючи враження про цілеспрямовану діяльність уповноважених державних органів з питань убезпечення держави і суспільства. Показником її несучасності (закостенілості) можна вважати пропозицію щодо підготовки так званого "паспорту загроз національній безпеці". У випадку його розробки й затвердження неповоротка система національної безпеки України імітувала б безпекову діяльність тільки стосовно закріплених у паспорті загроз, ігноруючи при цьому інші деструктивні імпульси, адресовані державі й суспільству, які могли бути несподіваними, нестандартними, алогічними. Як це видно з позицій сьогодення, загроза війни росії проти України на сторінках такого документу була б відсутньою.

Безпекова діяльність України в умовах протидії російській агресії (2014 р. — початок 2022 р.). На початку 2014 р. відбувся крах системи забезпечення національної безпеки України, побудованої на імітаційній основі. Система не змогла протидіяти російській агресії, націленій на Крим та східні райони Донеччини й Луганщини.

Керівниками державних органів (суб'єктами забезпечення національної безпеки), які залишили Україну, побоюючись відповідальності за антиукраїнську діяльність чи злочинну бездіяльність, спрямовану проти національних інтересів України, у лютому–березні 2014 р. стали Президент України, Прем'єр-міністр України, перший віце-прем'єр-міністр, голова Верховної Ради, Генеральний прокурор, голова Національного банку, міністри оборони, внутрішніх справ, доходів і зборів, енергетики та вугільної промисловості, освіти і науки, аграрної політики та продовольства, охорони здоров'я України, голова Служби безпеки, секретар Ради національної безпеки і оборони, деякі інші можновладці. Система забезпечення національної безпеки виявилась знищеною не лише за змістом (антиукраїнська діяльність), а й формальними підставами (втеча її керівників за кордон) [21, с. 76–77].

За підсумками 2014 р. Україна втратила 7% території (АР Крим, м. Севастополь, а також ОРДЛО), близько 20% ВВП, 407 км державного кордону. На той момент загинуло більше 12 тис. громадян України. Понад 1,6 млн. громадян стали біженцями. Як зазначалось у Стратегії національної безпеки

України від 26.05.2015 р., "прагнучи перешкодити волі Українського народу до європейського майбутнього, росія окупувала частину території України — Автономну Республіку Крим і місто Севастополь, розв'язала воєнну агресію на Сході України та намагається зруйнувати єдність демократичного світу, … підірвати основи міжнародної безпеки та міжнародного права, уможливити безкарне застосування сили на міжнародній арені" [16].

За таких умов в Україні стався безпеково-самоорганізаційний парадокс, значення якого важко переоцінити: суб'єкт забезпечення національної безпеки — громадяни України, — який в Законі "Про основи національної безпеки України" 2003 р. формально був згаданий на останньому місці, виявився фактичним рятівником своєї Вітчизни. Громадянське суспільство проявило себе як сила, що зірвала московські плани розчленування України на "Малоросію" та "інші" регіони. Свідченнями цього стали: стрімке, практично миттєве виникнення низки добровольчих частин і підрозділів та їх практичне застосування на Сході України (часто в ініціативному порядку); активне формування сил місцевої самооборони у регіонах, що могли опинитись на шляху подальшого просування російсько-сепаратистських сил; волонтерський рух, що взяв на себе функції матеріально-технічного, медичного, продовольчого та ін. забезпечення воюючих частин в умовах фактичної відсутності офіційного "Тилу Збройних Сил"; організація каналів обміну полоненими, які доповнили відповідні державні механізми або ж діяли самостійно; розгортання мас-медійних центрів, структур інформаційного спротиву пропагандистським впливам противника; відкриття центрів психологічної та соціальної реабілітації учасників АТО; організація антиросійських виступів української діаспори; імплементація цінностей патріотизму в духовно-культурне життя наявних суспільних верств (насамперед підростаючого покоління) в усіх без винятку регіонах України.

За цими безпеково-оборонними діями слід бачити глибинне явище історичного значення — збройно-силову реакцію громадянського суспільства на загрози й небезпеки, що загрожують існуванню незалежної і суверенної України. "Моментом істини" стала анексія Криму російськими збройними формуваннями, яка не отримала гідної відповіді з боку державних силових структур. Громадянське суспільство, яке у загрозливих ситуаціях соціально-політичної еволюції відрізняється підвищеною чутливістю сприйняття соціально-політичних небезпек порівняно з державними органами, миттєво відреагувало на високу ймовірність перенесення кримського сценарію на інші регіони України. Реакцією став силовий захист базових цінностей Українського народу, навіть в умовах неефективної діяльності (а то й прямої бездіяльності чи зради) офіційної держави [21, с. 77].

Відповідь на активізацію безпекового потенціалу громади слід шукати у правічному воєнному потенціалі українства, який в усі історичні часи був основою прагнень народу здобути незалежність [12, с. 213]. "Воююча Україна" стала атрибутом не лише князівських, королівських, козацьких, радянських часів, а й даністю XXI ст.

Громадою було запропоновано розширене розуміння сенсу національної безпеки. Якщо раніше під нею пропонувалося розуміти багатократно повторений у різних державних нормативно-правових актах стан захищеності національних інтересів, то після подій 2013–2014 рр. — стан захищеності як національних інтересів, так і національних цінностей. Інтереси (цілі діяльності) та цінності (морально-вартісні надбання вищого ґатунку, перевірені та накопичені багатьма поколіннями) стали співзвучними та взаємодоповнюючими. Проте якщо національні інтереси можуть варіюватися залежно від конкретно-політичної ситуації у державі та довкола неї, то національні цінності були, є й надалі залишатимуться інертними (менш залежними від поточної кон'юнктури) маркерами якості державотворчого процесу, в тому числі націєбезпекотворення. Формула "держава — національні інтереси — національна безпека як стан їх захищеності" доповнилася формулою "громадянське суспільство — національні цінності — національна безпека як стан їх захищеності". Виявилося, що спільної безпекової мети можна досягнути у спосіб, який єднає державне й суспільне.

За активного сприяння громадянського суспільства Україна вийшла на комбіноване розуміння націєбезпекової діяльності. Її суб'єктами виступають як держава, так і громадяни та їхні об'єднання. Сектор безпеки і оборони, необхідність створення якого на рівні концептуального документу була проголошена у 2016 р., постає як комбінований механізм забезпечення національної безпеки, що передбачає активну взаємодію державних органів (влади, політичної системи, легітимних збройних формувань) та структур громадянського суспільства, що опікуються аналітичним, освітньо-науковим, інформаційно-медійним, патріотично-виховним, а за потреби — і збройним доповненням державних зусиль.

Використовуючи "мілітарний протуберанець" громадянського суспільства 2014 р., Українська держава отримала дорогоцінну паузу, необхідну для повернення політичної системи у конституційно визначені умови існування включно з вирішенням нагальних безпеково-оборонних завдань. 25.05.2014 р. були проведені президентські вибори, 26.10.2014 р. — парламентські, 25.10.2015 р. — місцеві.

У Стратегії національної безпеки України від 26.05.2015 р. вперше у нормативно-правовій базі з питань забезпечення національної безпеки зазначалось: Україна, реалізуючи політику національної безпеки, захищатиме свої фундаментальні цінності — незалежність, територіальну цілісність, суверенітет, гідність, демократію, людину, її права і свободи, верховенство права, забезпечення добробуту, мир та безпеку [16].

У 2015 р. групою вітчизняних експертів було проведено дослідження "Аналіз державної політики у сфері національної безпеки і оборони" з метою аналізу причин провальних дій суб'єктів забезпечення національної безпеки України на початку загострення воєнно-політичної ситуації в Криму та на Донбасі [22, с. 266]. До причин низької ефективності системи забезпечення національної безпеки України було віднесено такі.

1) Ця система практично протягом усього довоєнного періоду будувалась за радянськими лекалами на основі Воєнної організації держави, яка була сформована на початку 90-х років шляхом «механічної» трансформації радянських збройних формувань (структур) в аналогічні формування (структури) незалежної України. Їх деідеологізація була поверховою. Віднесення РФ до можливих воєнних противників України понад два десятиріччя блокувалось на рівні державного керівництва.

2) Формування системи відбувалось під тиском та контролем інших держав, для яких просування власних інтересів було першочерговим завданням. Найбільш переконливим прикладом нав'язаного Україні зовнішнього воєнно-політичного рішення, яке багато в чому спричинило російсько-українську війну, стало примусове ядерне роззброєння України першої половини 90-х років, до чого доклали зусиль не лише РФ, а й США, Велика Британія, інші постійні члени РБ ООН.

3) Політичне керівництво України упродовж всього періоду незалежності відносило безпекові питання до другорядних. Перша Стратегія національної безпеки України була розроблена в період перебування на посаді лише третього Президента України. Всі Стратегії (загальною кількістю 4) готувались із запізненням та містили значну декларативну складову.

З урахуванням цього та інших аналітичних матеріалів було підготовлено та прийнято стали Закон України "Про національну безпеку України" від 21.06.2018 р. [23], який змінив правову розробку 15-річної давнини — Закон України "Про основи національної безпеки України" (2003 р.). Іншими важливими, хоча й запізнілими в політичному часі документами стали Стратегія розвитку оборонно-промислового комплексу України від 20.08.2021 р. [24], Стратегія воєнної безпеки України від 25.03.2021 р. [25], Стратегія кібербезпеки України від 26.08.2021 р. [26], Стратегія зовнішньополітичної діяльності України від 26.08.2021 р. [27], Стратегія інформаційної безпеки від 28.12.2021 р. [28], Стратегія забезпечення державної безпеки від 16.02.2022 р. [29], деякі інші документи.

На жаль, "безпековий лікнеп" України виявився надто затягнутим у часі та довіреним політичним силам, що не розуміли сутності національної безпеки та зневажали нею або калькували безпекові підходи сусідньої держави. Каталізатором безпекового мислення та безпекової діяльності України стала російсько-українська війна.

Безпекова діяльність України в умовах відсічі російській широкомасштабній агресії (після 24.02.2022 р.). Упродовж часу зосередження російських військ довкола кордонів України (2021 — 23.02.2022 р.) воєнно-політичне керівництво забезпечувалось достатньою кількістю інформації щодо ескалації воєнної загрози з боку РФ. Попередження на адресу України про наближення російського вторгнення постійно звучали від представників США, НАТО, впливових західних медіа. Разом з тим, упродовж 2021 р. питання своєчасного реагування України на загрозу російського вторгнення у діяльності державних органів не домінували. Легітимні владні структури

України були зосереджені на виконанні конституційно визначених обов'язків у режимі мирного часу.

24.02.2022 р. відбулось широкомасштабне вторгнення російських військ в Україну. Перед Україною постала реальна небезпека силового знищенням державності, фізичної ліквідації державного керівництва та патріотично налаштованих прошарків населення, руйнування національної ідентичності. За таких умов Президент України організував діяльність органів влади, відповідальних за національну безпеку і оборону — РНБОУ, Верховну Раду України, Кабінет Міністрів України, органи виконавчої влади, сектор безпеки і оборони, ОПК, інші державні структури, а також органи місцевого самоврядування. Пропозиції щодо організації загальноукраїнського опору ворогу з боку глави держави прозвучали на адресу громадянського суспільства — громадських об'єднань та добровольчих формувань відповідно до Закону України від 16.07.2021 р. "Про основи національного спротиву" [30].

24.02.2022 р. у зв'язку зі збройною агресією РФ проти України, що загрожувала її державній незалежності та територіальній цілісності, для забезпечення стратегічного керівництва ЗС України, іншими військовими формуваннями та правоохоронними органами глава держави утворив Ставку Верховного Головнокомандувача та затвердив її персональний склад [31].

Особливостями застосування РО МО України під час відсічі збройної агресії РФ у 2022-2025 рр. стали: рішення Президента України покласти на начальника ГУР МО України основну роль у координації діяльності розвідувальних органів нашої держави; виконання ГУР МО України ролі основного інформаційного хабу, до якого стікається вся важлива розвідувальна інформація від розвідувальних органів та інших складових сектору безпеки і оборони держави; залучення РО МО України до забезпечення реалізації санкційної політики стосовно фізичних, юридичних осіб, організацій та країн, які підтримують збройну агресію РФ проти нашої держави та ін.

Із запізненням, лише на етапі відсічі російській збройній агресії проти України постали питання щодо розуміння сутності національної безпеки України в умовах воєнного стану, параметрів її забезпечення, нормативно-правового обґрунтування тощо. Відповіді на них прозвучали як з боку державних структур, так і наукової спільноти.

Національна безпека в умовах воєнного стану являє собою такий стан захищеності особистості, суспільства і держави, коли їхній захист мирними (ординарними) способами є неможливим у зв'язку із збройним нападом на країну або через реальну загрозу такого нападу. Це зумовлює необхідність уведення особливих умов правового регулювання правовідносин, яким властиві суттєві правообмеження, поширювані на права людини, та розширення повноважень органів публічної влади, що має чітко обумовлений у часі (строковий) характер [32, с. 128]. Воєнний стан у свою чергу стає особливим правовим режимом гарантування (поновлення) або сприяння національній безпеці в умовах реальної або потенційної збройної агресії. Запровадження воєнного стану відіграє низку соціально вагомих функцій, які в умовах

мирного часу є малопомітними або відсутніми. Такими функціями є: правозахисна (організація відсічі зовнішній агресії), превентивна (запобігання зовнішньому втручанню у внутрішні справи держави), стабілізаційна (підтримання конституційного ладу, забезпечення територіальної цілісності та суверенітету держави), стимулююча (формування сприятливих умов для сталого розвитку національної економіки, суспільства та країни в цілому).

Конституційний Суд України у Каталозі юридичних позицій Конституційного Суду України (за рішеннями, висновками) відзначив: "згідно з приписами частини першої статті 17 Конституції України в умовах воєнного стану захист суверенітету і територіальної цілісності України, забезпечення її економічної, інформаційної безпеки є не лише найважливішими функціями держави, справою всього Українського народу, а й невіддільною умовою збереження української державності як такої" [33].

Верховний Суд України в Огляді від 03.05.2023 р. "Особливості застосування принципу національної безпеки в умовах воєнного стану в Україні" зазначив наступне [34]: в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень. При цьому не можуть бути обмежені права і свободи, передбачені статтями 24, 25, 27–29, 40, 47, 51, 52, 55–63 Конституції України; винятками є право на приватність (ст. 32), свобода слова (ст. 34), право на об'єднання у політичні партії та громадські організації (ст. 36, 37), право на мирні зібрання (ст. 39), право на страйк (ст. 44). Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; міжнародні стандарти застосування принципу національної безпеки мають базуватися на нормах Європейської конвенції про захист прав людини і основоположних свобод; термін "безпека" в Конституції України згадується більше 30 разів. Можна виділити чотири основні сфери застосування принципу національної безпеки: захист суверенітету, територіальної цілісності України, її економічної та інформаційної безпеки.

На основі цих юридичних норм та роз'яснень, новими реаліями забезпечення національної безпеки України після в умовах відсічі російській агресії стали динамічні зміни в правовому регулюванні безпекових правовідносин, масштабні реорганізації в державних органах, на які покладено виконання безпекових функцій, перегляд їх завдань і повноважень, створення нових органів державного управління (згаданої вище Ставки, а також обласних військових адміністрацій). Серед законодавчих нормативів національної безпеки стали превалювати імперативні приписи зобов'язального або заборонного характеру. Одночасно знизились кількість та рівень дії правових норм дозвільного або уповноважувального характеру. Воєнний стан став особливим правовим режимом гарантування національної безпеки в умовах

реальної збройної агресії. За таких умов об'єктивно відбулось посилення ролі держави, виправдане відновлення етатизму в межах мобілізаційної моделі функціонування політичної системи.

У структурі безпекового законодавства виокремились наступні блоки: а) нормативно-правові акти, що обумовлюють необхідність запровадження режиму воєнного стану; б) нормативно-правові акти, що деталізують окремі положення безпеково-оборонних заходів, стосуються повноважень державних органів, органів місцевого самоврядування в умовах воєнного стану; в) нормативно-правові акти, що стосуються обмеження прав і свобод людини, покладення на людину додаткових юридичних обов'язків з питань національної безпеки в умовах воєнного стану; г) нормативно-правові акти, що передбачають юридичну відповідальність за правопорушення у сфері національної безпеки в умовах воєнного стану [35].

Невідкладного характеру набули питання щодо фінансування безпекових і оборонних потреб держави шляхом перерозподілу внутрішніх бюджетних видатків та фінансових потоків із-за кордону, оптимального використання Збройних Сил та інших структур сектору безпеки і оборони, забезпечення їх мобілізаційного розгортання, реабілітація оборонно-промислового комплексу держави (з урахуванням втрат і збитків воєнного періоду), формування науково-дослідних лабораторій, орієнтованих на модернізацію наявних систем озброєнь і військової техніки та розробку інноваційних систем зброї.

Критично гострого вигляду набула проблематика забезпечення інформаційної безпеки держави і суспільства, їх захисту від цілеспрямованих інформаційних (інформаційно-психологічних) впливів з боку російської пропаганди. За цим проступала загальнонаціональна потреба не допустити панічних настроїв широких верств населення, негативного сприйняття ними державно-управлінських рішень, втрати довіри до органів державної влади. Дотичною до національної інформаційної сфери виявилась сфера кібернетична, від технічної досконалості та оперативної стійкості якої залежали механізми підтримки функціональної спроможності ключових суспільних сфер (воєнної, енергетичної, транспортної, соціальної), численні бази даних, а також інформаційні обміни міжнародного рівня, всередині держави, між державою і суспільством, різними соціальними групами та індивідами.

Зусиллями державних органів було сформовано кілька форматів міжнародної підтримки боротьби України з російською агресією. 12.11.2022 р. Президент України В. Зеленський оприлюднив "формулу миру". Для її реалізації були проведені зустрічі послів, акредитованих в Україні, а також радників з питань національної безпеки. У 2023 р. Генеральна Асамблея ООН проголосувала за резолюцію про "Принципи Статуту ООН, що лежать в основі досягнення всеосяжного, справедливого та міцного миру в Україні". 15-16.06.2024 р. у Швейцарії відбувся Глобальний саміт миру — міжнародна зустріч лідерів держав заради мир в Україні.

Об'єктивною реальністю стало формування потужної проукраїнської позиції у правлячому політикумі США, Великої Британії, Польщі, держав Балтії, інших демократичних країн. Свідченням воєнно-технічної допомоги Києву з боку демократичних країн стала Консультативна група з питань оборони України (група «Рамштайн»). Низка країн визнали дії РФ в Україні геноцидом та запропонували оголосити РФ державою-спонсором тероризму.

У загальній панорамі міжнародної підтримки України слід виокремити британську та американську складові. Представники Великої Британії та США у 2022 р. заявили про підтримку України до переможного завершення російсько-української війни. Британія додатково заявила про готовність стати гарантом безпеки України в майбутньому.

Новим складником забезпечення національної безпеки України в умовах війни стала проблема формування дієвих механізмів запобігання та протидії корупції. Фінансові, матеріальні, інформаційні та інші ресурси України на основі активної міжнародної допомоги, спрямованої на посилення протидії російській агресії, а також оперативність їхнього використання значно зросли. При цьому послабилась ефективність державного обліку та контролю за використанням новоотриманих ресурсів. Слід було очікувати нових інформаційно-психологічних атак РФ, спрямованих на звинувачення України у неспроможності розпорядитися іноземною допомогою й навіть перепродажу зброї та військової техніки міжнародним терористам. Це стало реальністю у 2022—2023 рр., коли російська пропаганда на основі "розвінчування" українських "зловживань" намагалася послабити підтримку України з боку демократичних держав Європи і світу.

Паралельно з цим у фаховому дискурсі вказується на сфери забезпечення національної безпеки, якими Україна до російського широкомасштабного вторгнення практично не опікувалася. Йдеться про ментальну безпеку українського суспільства, його переконаність у національній самодостатності, рішучу відмову від "малоросійського" або "новоросійського" тлумачення витоків та перспектив розвитку українства, яке в російській історичній думці подається як "південно-західне відгалуження єдиного великоросійського народу" [36, с. 148].

На основі викладених вище матеріалів доцільно сформулювати припущення, істинність якого підтверджена безпековою практикою не лише України, а й інших демократичних країн: формат національної безпеки не може бути детально прописаний заздалегідь. Майже завжди слід очікувати непередбачені впливи на систему національної безпеки, що можуть бути вербально позначені як "невизначеність" [37].

Категорія невизначеності в безпековій діяльності сучасних держав. Феномен невизначеності має підтвердження у вигляді політичного досвіду більшості сучасних країн. Розглянемо різні варіанти її прояву, які прямо чи опосередковано впливають на національну безпеку.

Невизначеність 1. Національна безпека з моменту публічної артикуляції її засад на початку XX ст. традиційно сприймалася як стан захищеності

життєво важливих інтересів особистості, суспільства, держави, за якого забезпечувалися їх поступальний розвиток та мінімізація контр-спрямованих ризиків. Майже завжди "життєво важливі інтереси» варіативно представлялись як "національні інтереси", підживлювані "національними цінностями". Як національні інтереси, так і національні цінності отримували нормативно-правову фіксацію на сторінках відповідних нормативно-правових розробок — законів, стратегій, доктрин. Беззаперечними виглядали категорія "нації" як висхідний момент формулювання національних інтересів і цінностей.

Соціально-політичні трансформації останнього часу ставлять під сумнів вищість нації у загальному спектрі суспільних відносин. Нації не є константою соціогенезису, їхні статичні ознаки зміщуються, трансформуються, іноді зникають. Інтенсифікація міграційних потоків у вигляді рухів заробітчан, біженців, шукачів політичного притулку ставить під сумнів виключне становище націй як усталених одиниць соціально-політичного аналізу, що було властиве минулому століттю. Політична, етнічна, культурологічна теорії походження нації стають лише «частково справедливими», не відбиваючи усієї повноти соціальної динаміки. Доволі часто формальне проживання індивіда на території певної країни аж ніяк не засвідчує його повноцінну належність до місцевої нації. Індивідом можуть не сприйматися (відторгатися) інтереси й цінності нового соціального оточення, які (з точки зору формальних керівників держави перебування) визначаються як національні. Відбувається розмивання фундаментальних основ національної безпеки, до захисту якої умовний "мігрант Х" аж ніяк не готовий.

Виникає наступна суперечлива ситуація: на території конкретної держави-нації, яка довела свою стійкість у попередніх історичних випробуваннях, зараз дедалі частіше з'являються індивіди (соціальні групи), які не відчувають повноцінної належності до "нової батьківщини" та сфери її національної безпеки. У кількісному вимірі подібні групи невпинно зростають, опираючись на власні соціокультурні, мовні, релігійні, побутові та інші особливості. Як результат, у суспільно-політичних реаліях умовної "країни N" маємо національну безпеку "не для всіх". У неї не вписуються численні варіації індивідуальної (сімейної, родинної, кланової) життєдіяльності мігрантів, які не співпадають з державними підходами щодо забезпечення національної безпеки або спрямовуються проти них.

Невизначеність 2 проглядається у недостатній готовності правлячих еліт регулювати національну безпеку на основі "сферного" підходу. В Україні раніше звучали законодавчі приписи щодо забезпечення національної безпеки в усталених сферах — політичній (внутрішній та зовнішній), економічній, соціальній, воєнній, інформаційній, технологічній, духовно-культурній, екологічній, гуманітарній, у сферах безпеки державного кордону, цивільного захисту населення та ін. Останніми додатками до переліку сфер забезпечення національної безпеки стали сфери кібернетичної та міграційної безпеки, значення яких у конфліктних взаєминах сучасності невпинно зростає. Попри

намагання законотворців прописати максимальну кількість сфер на сторінках певного державного документу залишались суспільні ніші (сфери), які не потрапляли у визначений перелік. Ними, зокрема, були сфери конфесійної, морської, етнонаціональної, продовольчої безпеки тощо.

Отже, "сферна" диференціація феномену національної безпеки не враховує всього різноманіття соціального буття та необхідності його багатостороннього моніторингу. У сучасних умовах будь-який фрагмент фізичного, кібернетичного або духовного простору, де присутня людська діяльність може стати середовищем виникнення різноманітних загроз та державних і суспільних контр-дій відносно них. Відповідно, вузьке тлумачення небезпечних ситуацій у визначених законодавством сферах хоча й застосовується на практиці, проте поступається місцем комплексному баченню різнопланових загрозливих впливів, здатних проявитися в широкому діапазоні та підірвати заздалегідь створену "сферну" конструкцію безпеки.

Невизначеність 3 проглядається у різночитанні природи імпульсів, спрямованих проти неї. Задля конкретизації таких впливів у деяких країнах (зокрема пострадянських) широко використовуються терміни "виклики", "загрози", "небезпеки". Вважається, що їх основною відмінністю є інтенсивність деструктивного впливу на предмет національної безпеки: виклик може призвести до його часткової деформації, загроза — до руйнування, небезпека — до повного знищення без можливості наступного відновлення. Проте вичерпного змістовного роз'яснення цих термінів національні правові системи не наводять. У безпекових реаліях відбувається довільне змішування вказаних термінів. Зокрема деградація середовища безпеки різними авторами описується через довільно побудовані парні констатації: виклик — небезпека, загроза — виклик, загроза — небезпека тощо. Подібні вербальні конструкції додатково заплутують розуміння національної безпеки, посилюють непозначений (ірраціональний) компонент її еволюції. У діяльності з питань національної безпеки подібна вербальна недисциплінованість створює додаткові умови її суб'єктивного розуміння та практичного втілення.

Для виправлення ситуації останнім часом більш широко вживається західний термін "ризик" як універсальний змістовний еквівалент викликів, загроз та небезпек. Це допомагає більш адекватно окреслювати безпекову ситуацію, проте розширює межі суб'єктивізму в безпековій діагностиці.

Невизначеністю 4 в інструментальному забезпеченні національної безпеки є надмірна суб'єктивність процесу визначення структури, функціонального призначення та ресурсного забезпечення сектору безпеки і оборони як основного інструменту здійснення націєбезпечної діяльності в суспільних сегментах, де фізична (збройно-силова) активність людини поки що залишається домінантною.

Максимально лаконічно сектор безпеки і оборони описується як "всі силовики", створені демократичною державою та орієнтовані на убезпечення національних інтересів. Насамперед йдеться про збройні сили (армію),

поліцію, національну гвардію, пенітенціарні органи, служби безпеки, прикордонного захисту, надзвичайних ситуацій, розвідувальні органи та центри управління ними, деякі інші державні органи спеціального призначення. Окремі країни до цього переліку додають структури воєнно-промислового комплексу, а також громадські об'єднання, що опікуються безпековими й оборонними питаннями.

Отримуємо доволі розгалужений формат державних та громадських утворень, націлених на забезпечення національної безпеки. При цьому правлячий політикум одноосібно визначає "запас міцності" сектору безпеки і оборони, який залежить від кількості віднесених до нього збройних формувань (служб) та способів їх підготовки й застосування. Вимоги щодо уніфікації сектору безпеки і оборони у політично інтегрованих країнах (наприклад у НАТО) є доволі приблизними. Кожна країна, що входить до Альянсу, здатна проявити "безпеково-організаційну творчість" з метою створення силових структур, які, на погляд держави, оптимально відповідають поточним ризикам. Як наслідок виникає ситуація підвищеної складності у процесі налагодження взаємодії між секторами безпеки і оборони різних держав, оскільки формальна подібність силових структур різних країн розмивається специфікою національного мислення з безпекових і оборонних питань та національними пересторогами щодо потрібності/непотрібності віднесення того чи іншого органу до системи забезпечення національної безпеки.

Ситуація ускладняється з огляду на стійку симпатію автократичних систем до воєнної організації держави — аналога сектору безпеки і оборони у демократичних країнах. З подачі російського керівництва ідеологія домінування ВОД у політичних відносинах всередині країни та за її межами підтримується державами, які симпатизують російському режиму. Принципова різниця між секторами безпеки і оборони та воєнними організаціями держав полягає у наявності/відсутності всеохоплюючого демократичного контролю над силовими структурами та унеможливленні одноосібного використання державним лідером силових ресурсів держави. У демократичних країнах такий контроль є даністю, ознакою безпеково-оборонної культури нації. На противагу цьому в автократичних державах демократичний контроль є або формальним, або відсутнім. Виникає додаткова суспільна невизначеність: яким чином можливо налагодити взаємодію (тим більше співпрацю) секторів безпеки і оборони та воєнних організацій держав, які за своєю природою були й залишаються цивілізаційними антиподами? Одного разу це сталося (у виключних воєнно-політичних умовах Другої світової війни при формуванні антигітлерівської коаліції держав). Наступні 80 років світової історії, стержнем яких стала Холодна війна між геостратегічним Заходом і Сходом, засвідчили неможливість відтворення подібного формату міждержавних взаємин. В умовах сьогодення суспільна невизначеність як фактор впливу на безпекову й оборонну політику загострюється до політичної неможливості британсько-російської, американсько-китайської або білорусько-польської

співпраці у сфері посилення міжнародної безпеки шляхом формування та практичного застосування змішаних військових контингентів.

Невизначеністю 5 у контексті позадержавної підтримки безпекової і оборонної політики є неможливість завчасного визначення оптимуму державно-громадянської взаємодії з питань забезпечення національної безпеки в умовах мирного та воєнного часу. Суспільний досвід неодноразово продемонстрував здатність зацікавленої громади вирішальним чином впливати на політичну владу — коригувати державний курс, змінювати політичний режим, досягати персональних змін у правлячій еліті. Проте особливої чутливості державно-громадянська взаємодія набуває під час військових конфліктів (війн). Тут можливими стають два варіанти розвитку подій.

У випадку апелювання легітимної влади до необхідності збройного захисту національних інтересів і цінностей відбувається продержавна поляризація патріотично налаштованих структур громадянського суспільства з метою всебічної допомоги владі. Суспільство виступає ресурсом стійкості держави. За його ініціативою у форс-мажорних умовах стрімко виникають сили самооборони, добровольчі батальйони, підрозділи та частини територіальної оборони, які захищають державу разом зі збройними силами. До інших важливих проявів безпекової (оборонної) активності громади слід віднести волонтерські рухи, аналітичні осередки, медійні структури, значення яких було й залишається надзвичайно суттєвим. У такий спосіб проявляється потенціал національної стійкості, здатності суспільства до самоорганізації.

У випадку ліквідації (знищення) ворогом держави громада пропонує власні варіанти суспільного виживання включно з висуванням нових політичних лідерів та налагодженням альтернативних форматів політичної активності (включно зі збройною боротьбою проти ворожої сторони). Іншими словами, держава у випадку критично-руйнівного збройного впливу ворога тимчасово може не існувати. Проте суспільство залишається. Навіть суспільний фрагмент демонструє завидну живучість та орієнтується спочатку на відновлення якості власного існування, а потім — й на відновлення державності. Це доводить, що зріле громадянське суспільство, якому властиве глибинне розуміння національних цінностей та інтересів, в історичному часі стає основним замовником державотворчого проєкту. Відбувається відродження нації включно з реалізацією нею на зрілому етапі розвитку державно-громадянського суб-проєкту “національна безпека”.

Проте детально визначити наперед алгоритм громадянського впливу на державу в контексті спільного відстоювання безпекових й оборонних характеристик соціуму неможливо. Збройно-силовий експромт громадянського суспільства з цих питань завчасному плануванню не підлягає. Отримуємо додатковий різновид суспільної невизначеності з питань залучення громадянського суспільства у діяльність з питань національної безпеки.

Невизначеністю 6 виступає ступінь делегування суверенною державою безпекових повноважень міжнародним структурам, у назві яких присутнє

слово “безпека”. Широкомасштабна агресія РФ проти України унаочнила вражаючу слабкість більшості безпекових органів міжнародного рівня, які виявилися неспроможними запобігти російському вторгненню або мінімізувати його перебіг. Йдеться про Раду Безпеки ООН та ОБСЄ, міжнародно-регулятивний потенціал яких залишився в минулому столітті. Якщо взяти до уваги державу-агресора, то вона опинилась у схожій ситуації: у війні з Україною їй мало чим допомогла завчасно створена за російською ініціативою Організація Договору про колективну безпеку. Єдиний виняток — спрацювали механізми НАТО, заблокувавши перенесення бойових дій на територію Альянсу та запустивши процес його дев’ятого розширення шляхом вступу Фінляндії і Швеції.

Новітня історія України *збагатила перелік невизначеностей,* що стосуються національної безпеки і оборони, невизначеністю гібридної війни, яка у структурному, функціональному, ресурсному та інших вимірах є доволі складною імпровізацією. Мета гібридної війни нічим не відрізняється від мети гарячої війни — послаблення або знищення держави-ворога. Сутність гібридного різновиду війни полягає у цілеспрямованому створенні (гібридизації, схрещуванні) нестандартних ударних форматів — традиційно-збройних, інформаційних, дипломатичних, економічних, екологічних, мережевих, кібернетичних, громадянських, партизанських, терористичних, їх вибірковому або масованому використанні [38, с. 12—13]. Відбуваються: поєднання конвенційних та неконвенційних бойових дій, мілітарних, квазімілітарних, дипломатичних, санкційно-обмежувальних, фінансових, енергетичних, торговельних, технологічних, кібернетичних та інших форм боротьби; розширення кола учасників (військовослужбовці, учасники приватних армій, найманці, партизани, ополченці, терористи тощо); «розмитість» моменту початку (без вручення ноти про оголошення війни) та закінчення (без підписання акту про капітуляцію). Особливого значення набуває інформаційна (інформаційно-психологічна, пропагандистська) боротьба із застосуванням усіх доступних способів впливу на індивідуальну й групову свідомість тих, з ким ця війна ведеться.

Стає зрозумілим, що кількість невизначеностей у заплутаному форматі гібридної війни є надмірною, не підлеглою лінійному аналізу на кшталт “фронт — тил”, “друг — ворог”, “невтручання — колабораціонізм” тощо. Конче потрібним стає нове безпекове мислення, побудоване на обробці астрономічних масивів інформації та виокремленні з них раціональної складової, здатної відповісти на гострі поточні питання щодо національної безпеки та збройної боротьби як її складової.

Феномен невизначеності як чинник коригування політики національної безпеки. Комбінація невизначеностей та залежних від них загроз, з якими людство зіткнулося на початку XXI ст., сприймається як унікальна, раніше невідома й особливо небезпечна. Сучасна наука з метою розуміння природи соціальних ситуацій, ознаки яких є не- або малозрозумілими, а наслідки спроможні стати особливо руйнівними — пропонує нові концептуальні

підходи до осмислення суспільних відносин в умовах невизначеності. Одним з них є концепт "VUCA-світу", де Volatility означає мінливість, Uncertainty — невизначеність, Complexity — складність, Ambiguity — багатозначність [39, с. 43—47]:

Volatility (мінливість, нестабільність, нестійкість) — ситуація змінюється швидко й хаотично; на основі наявних даних не можна передбачати наступну ситуацію або планувати подальші дії;

Uncertainty (невизначеність) — відсутні передбачуваність, планомірність та розуміння причинно-наслідкових зв'язків між причинами, проблемами та подіями, формально рознесених у просторі й часі; майбутнє стає непередбачуваним через неможливість/обмеженість використання попереднього досвіду; зростає імовірність руйнівних змін соціального середовища;

Complexity (складність) — спостерігається лавиноподібне накопичення суперечливих фактів, оцінок, пропозицій; наслідками змішування різнопланових духовних утворень (позицій, оцінок, пропозицій) стають хаос, плутанина, безлад у соціальних взаєминах, які протидіють впорядкованим структурам та суттєво ускладнюють управлінську діяльність;

Ambiguity (багатозначність) — домінують суб'єктивне тлумачення ситуації та некоректне сприйняття проблеми, наслідком чого стає поверховість у ставленні до неї; різними авторами довільно змішуються вербальні формули, що описують проблему; як наслідок просторово-часовий фрагмент соціальної еволюції не підлягає лінійному моніторингу на основі однозначних суджень.

Попри важливість кожного із названих елементів основним складником VUCA-світу вважається невизначеність, яка трактується як неоднозначність, неповнота, нечіткість, непередбачуваність розвитку ситуації, управління якою з боку зацікавленого суб'єкта можливе лише на частковій основі або взагалі неможливе. Будучи складником більшості соціальних систем і процесів, невизначеність відбиває обмеженість свідомої участі людини у надперсональних процесах та існує незалежно від поточного розуміння їх сутності й наслідків прояву. При цьому невизначеність слід відрізняти від помилковості та недетермінованості. Яскравим прикладом формування політики на основі помилковості є військова кампанія росії проти України, розпочата у 2014 р. та розрахована на короткий час. Кампанія базувалась на основі низці припущень, непродуманих та надто оптимістичних для російського керівництва. Ігнорування можливості таких помилок створило невизначеність, яка призвела до недооцінки з боку і російських, й західних політиків та експертів потенціалу стійкості та опірності України напередодні російського вторгнення. Якщо узагальнити, то невизначеність у більшості випадків є результатом відсутності інформації, необхідної для прийняття рішень, або відсутності довіри до такої інформації та джерел її походження.

Відповідями на виклики VUCA-світу, здатними допомогти суб'єкту соціального управління (державі) подолати невизначеності та ефективно

діяти у недостатньо зрозумілих ситуаціях, пропонується віднести протилежну версію VUCA-концепту [40], де:

бачення (Vision) — чітке сприйняття та розуміння довгострокового напрямку руху, що дозволить організації пережити "струс". Бачення є важливим кроком до стабілізації ситуації, яке здатне надихнути всі зацікавлені сторони до перетворень. Похідними від бачення опціями стають чіткість поставленої мети; віра, яка підкріплена фактами та доказами; узгодженість та зосередженість щодо знаходження взаємозв'язків, трендів та закономірностей впливу сторонніх факторів;

розуміння (Understanding) — постійний моніторинг очікувань з боку об'єктів впливу; дослідження нових ідей та їх відображення в практичній діяльності; здатність до співпраці; вміння реагувати на конструктивну критику; володіння новими IT-технологіями; розуміння поведінки людей в ситуації стресів і навантажень; розуміння мотивів індивідуальної діяльності;

креативність / ясність (Creativity / Clarity) — вміння спрощувати; застосування системного мислення, заснованого на глобальному баченні результату, розумінні взаємодії і взаємозалежності елементів системи; використання інтуїції; застосування міждисциплінарних знань; критичність сприйняття подій; гнучкість до впровадження змін; націленість на інновації в будь-якій галузі та готовність втілювати в життя інноваційні підходи;

гнучкість, спритність, рішучість, швидкість, жвавість (Agility) — швидкість і гнучкість виконання процесів, що сприяє підвищенню ефективності функціонування організації; впевненість у необхідності інновацій, пошуку нових оригінальних шляхів вирішення всіх питань, поліпшення процесів; рішучість у прийнятті рішень; інноваційність, формування мережевих зв'язків; постійне вдосконалення.

У даному випадку теж звучить акронім VUCA. Проте тут він пропонує відповіді на питання, продиктовані невизначеністю. Чинник VUCA може і має бути врахований в теорії і практиці національної безпеки. Його використання не має стримуватись ні "сфер ними" кордонами, ні "паспортами загроз", ні іншими статичними елементами сприйняття середовища національної безпеки.

Зараз пропонуються три основні способи управління невизначеністю: 1) кількісний аналіз ситуації, яка містить компонент невизначеності; раціональне сприйняття відомого, зрозумілого, прорахованого, що звужує простір об'єктивації невідомого або невизначеного. Ratio має переважати irratio, що є умовою прийняття зважених політичних рішень; 2) локалізація невизначеності. Її повне вилучення з державно-управлінської діяльності є неможливим. Проте владні центри цілком спроможні пояснити свої дії на основі зрозумілої суспільно-політичної логіки, страхуючись при цьому від ймовірних "чорних лебедів"; 3) планування заходів щодо зменшення невизначеності. Зокрема, пропонується: контролювати інформацію з метою підвищення її достовірності, а також недопущення маніпуляцій; чітко визначати проблеми, цілі й наслідки перед прийняттям рішення, в ході його

виконання та після завершення; формувати ширшу та більш активну дослідницьку спільноту; залучати додаткові (альтернативні) наукові, науково-аналітичні та медійні установи до опрацювання безпекової проблеми з елементами невизначеності.

На основі цього можна зробити такі висновки щодо доцільності внесення принципових змін до формування й реалізації політики національної безпеки з урахуванням впливу невизначених чинників:

раптові й непередбачувані зміни безпекового середовища вимагають більшої гнучкості під час формування і реалізації державної політики; шаблонність мислення, побудована на минулому досвіді, обмежує цю гнучкість;

необхідність реагування на ситуацію невизначеності потребує уточнення значення нації як об'єкту захисту, перегляду ієрархії національних інтересів, пошуку нового балансу між національними цінностями та потребами забезпечення національної безпеки і стійкості;

доцільним є впровадження більш гнучких, але зрозумілих підходів до визначення напрямів забезпечення національної безпеки, з урахуванням особливостей трансформації ризиків у сучасних умовах;

продовжується пошук оптимального складу сектору безпеки і оборони на національному рівні та шляхів оптимізації державно-громадської взаємодії у мирний і воєнний час;

зростає потреба у перегляді повноважень, делегованих національними урядами міжнародним безпековим організаціям, а також пошуку ефективних механізмів кризового врегулювання на міжнародному рівні;

формування і реалізація державної політики має здійснюватися на засадах адаптивного управління, що передбачає постійний моніторинг ситуації, виявлення нових трендів, ризиків і загроз, регулярний аналіз відповідності цілей і завдань державної політики змінам у безпековому середовищі;

з огляду на поширення нелінійних зв'язків у системі суспільних відносин потребують оновлення концептуальні підходи до оцінювання ефективності державної політики у сфері національної безпеки та розроблення інструментів оцінювання її відповідності принципам стійкості;

доцільним є інвестування у розвиток науки. Нової якості має набути безпекова прогностика, насамперед розробка нових способів (методик) прогнозування змін у сфері міжнародних взаємин та їх впливу на конкретні держави з метою зменшення потенціалу невизначеності в їх економічному, політичному, екологічному, духовно-культурному та іншому поступі.

ШІ як чинник осучаснення системи національної безпеки України. Сучасними здобутками щодо використання ШІ у безпековій сфері слід назвати [41]:

1. Автономні системи озброєння (АСО). Збройні системи з ШІ можуть самостійно ідентифікувати, відстежувати і вражати цілі з мінімальною участю людини, щоб мінімізувати ризики супутньої шкоди й одночасно підвищити ефективність військових операцій.

2. Системи спостереження та розвідки. Алгоритми ШІ можуть використовувати величезні обсяги даних спостереження, такі як зображення, аудіопотоки і радіолокаційні сигнали, щоб виявляти закономірності, відхилення і відстежувати цілі для інформування військового командування в режимі реального часу.

3. Системи розпізнавання та класифікація цілей. ШІ може бути використаний для ідентифікації і класифікації об'єктів, таких як озброєння, бойова, боєприпаси, бойова та інша техніка і особовий склад, для більш швидкого і точного виявлення і ураження цілей.

4. Системи аналізу й прогнозування загроз. Системи ШІ можуть використовувати історичні дані, поточну інформацію, враховувати інформацію про навколишнє середовище для точного прогнозування потенційних загроз або вразливостей та вжиття превентивних кроків для протидії ризикам.

5. Системи логістики та управління ланцюгами постачання. Технології ШІ можуть допомогти логістичним операціям, оптимізуючи планування маршрутів, контроль запасів, розподіл ресурсів, підвищуючи ефективність і знижуючи витрати.

6. Системи забезпечення кібербезпеки, здатні виявляти й нейтралізувати кібератаки, захищаючи критично важливу військову інфраструктуру і мережі.

7. Системи радіоелектронної боротьби. Технології ШІ дозволяють аналізувати перехоплені сигнали з каналів зв'язку та інші форми електронного зв'язку, щоб визначити місцезнаходження ворожих позицій, вивести з ладу ворожі комунікаційні мережі та отримати тактичну перевагу над противником.

8. Системи симуляції та навчання. Симуляції на основі ШІ створюють реалістичні умови для тренувань військових, дозволяючи їм відпрацьовувати бойові сценарії і набувати нових навичок.

9. Системи підтримки прийняття рішень. Технології ШІ можуть використовуватися для аналізу великих масивів даних й надання рекомендацій державним управлінцям у сфері національної безпеки і оборони для аналізу, стратегічного планування та вироблення оптимальних практичних рекомендацій.

Впадає в очі асиметричність наявних можливостей ШІ: пп 1, 2, 3, 5, 7, 8 відповідають потребам збройної боротьби на тактичному й оперативному рівнях. Лише пп 4, 6, 9 можуть бути віднесені до більш високого рівня забезпечення безпеки, яка наближається до національного масштабу.

До цього варто додати алгоритми застосування ШІ у ситуаціях, пов'язаних з ідентифікацією конкретних індивідів. Йдеться про опції розпізнавання голосу, виявлення помилок в людських діях, розшифровку емоцій тощо. Називаються професії, які можуть зникнути а умовах подальшого технологічного удосконалення систем ШІ. Йдеться про психологів та психотерапевтів, медсестр, бізнес-консультантів, журналістів-розслідувачів.

Фахівцями НАТО визначено напрями розвитку науки й технологій, які потенційно матимуть вплив на розвиток безпеки і оборони на перспекти-

ву до 2040 р. Це технології великих даних, автономні системи, квантові, космічні та гіперзвукові технології й біотехнології. Основними характеристиками, які визначатимуть більшість ключових військових технологій, стануть [42]:

інтелектуальність — використання інтегрованого ШІ, орієнтованого на знання аналітичних можливостей людського інтелекту, та симбіотичного ШІ для забезпечення одночасного застосувань різних «проривних» технологій;

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

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

цифровізація — цифрове поєднання людських, матеріальних та інформаційних областей для досягнення визначеної мети.

У передових країнах вже сьогодні існують зразки озброєнь, які використовують можливості ШІ. Так, у 2020 р. у ВПС Великої Британії розгорнуто систему розвідки, спостереження й цілевказівки "Істар" (ISTAR — Intelligence Surveillance Target Acquisition and Reconnaissance). Система забезпечує виявлення наземних та морських об'єктів та спостереження за їхнім пересуванням. Іншим важливим напрямом розвитку військових систем, обладнаних ШІ, є централізоване планування і координація проведення військових операцій різного масштабу в повітряному, космічному, кібер-, морському та наземному просторі під назвою "багатосферне управління і контроль" (Multi-Domain Command and Control — MDC). Шляхом збору та обробки всієї доступної інформації, що надійшла з різних джерел, пропонується створювати інтегроване джерело інформації (глобальну оперативну картину), на основі якої командирам різного рівня будуть автоматично пропонуватися найбільш ефективні варіанти дій для досягнення поставлених цілей [43].

Реагуючи на світові тренди, Кабінет Міністрів України у 2020 р. прийняв Концепцію розвитку штучного інтелекту в Україні, яка визначила дев'ять пріоритетних сфер: освіту, науку, економіку, кібербезпеку, оборону, інформаційну безпеку, державне управління, правове регулювання та етику, правосуддя [44]. В контексті оборони слід забезпечити використання технологій ШІ у системах командування та управління, озброєння та військової техніки, збору та аналізу інформації під час ведення бойових дій, аналізу/розвідки, підтримки проведення розвідувальних заходів, обробки картографічної інформації, протидії кіберзагрозам у сфері оборони, що базуються на швидкому виявленні кібератак, імітаційного та когнітивного моделювання бойової обстановки, когнітивного аналізу спроможностей військових підрозділів.

Як недолік, доводиться констатувати, що на сторінках Концепції йдеться про інформаційну безпеку та кібербезпеку. Національна безпека як надважливий напрям (сфера) державної політики у документі не згадана.

У 2023 р. Міністерство цифрової трансформації України представило Дорожню карту з регулювання ШІ в Україні [45]. У 2024 р. вийшла Біла книга, яка більш детально описує підхід до регулювання ШІ в Україні. Проте і в драному випадку тема національної безпеки не прозвучала.

Отже, на сучасному етапі у структурі національної безпеки України беззастережна першість об'єктивно належить воєнній безпеці, що пояснюється чинником російсько-української війни. Державні органи, конкретні фахівці, представники зацікавленої громади мають зосередитись на виконанні Концепції розвитку штучного інтелекту в Україні 2020 р. (частина Оборона).

У перспективі найближчих років документ має бути видозмінено. Доцільним уявляється розробка та прийняття Стратегії розвитку штучного інтелекту в Україні, узгоджену з іншими державними стратегіями з питань забезпечення національної безпеки. Термін "штучний інтелект" має бути внесений у законодавство України з питань національної безпеки та наступні Стратегії національної безпеки України.

Висновки. Діяльність з питань національної безпеки України є складовою державотворчого процесу, яка не має історичних витоків та вдалого досвіду практичної реалізації. Діяльність з питань забезпечення національної безпеки України слід розділити на імітаційний етап 1991—2014 рр. (національна безпека державними органами проголошувалася) та сутнісний етап, що розпочався після 2014 р. (національна безпека виборюється спільними зусиллями держави та громадянського суспільства, а ставлення до неї виступає маркером про- або ж антиукраїнської позиції учасників політичного процесу).

Запропонований державою на початку 90-х років «вузький» підхід щодо розуміння національної безпеки України як стану захищеності її національних інтересів після Революції гідності 2013—2014 рр. змінився на більш розширений: національна безпека — це стан захищеності національних інтересів та національних цінностей, які є невіддільними.

Головним прорахунком України на імітаційному етапі розвитку системи національної безпеки став надмірний етатизм у визначенні її інституційних, структурно-функціональних, ресурсних, цільових та ін. характеристик. У центрі уваги правлячих сил більше двадцяти років перебувала Воєнна організація держави, яка реставрувала радянські підходи та копіювала досвід пострадянських диктатур. Євроатлантичний курс України вимагав відмови від ВОД на користь сектору безпеки і оборони, проте державотворчі еліти це зробили з великим запізненням.

Слабкість Української держави у питаннях забезпечення національної безпеки з усією очевидністю проявилася у 2014 р. після окупації РФ частини території України (АР Крим, м. Севастополь) та розв'язання воєнної агре-

сії на Сході України. Державна слабкість значною мірою була компенсована зусиллями громадянського суспільства (добровольчими батальйонами, волонтерським рухом, інформаційними мережами тощо), а також допомогою демократичних країн Заходу. Ключову роль у "заморожуванні" російської експансії 2014—2022 рр. зіграла українська громада, яка застосувала проти російського вторгнення низку підходів, у тому числі збройну протидію.

Проте компенсаційні можливості громадянського суспільства у сфері національної безпеки не можуть бути гарантом її достатності. Українська держава має здійснити необхідні перетворення, посилюючи статус головного безпекового суб'єкта, але опираючись на безпеково-оборонні можливості небайдужої громади. У випадку тривалої слабкості держави сумарна кількість небезпек, нав'язаних ззовні, набуде критичного вигляду та призведе до ліквідації Української державності.

У сучасному світі невизначеність є основним чинником впливу на формування та реалізацію державної політики у сфері національної безпеки. Ускладняються характер проблем, що потребують уваги з боку держави, множаться невизначеності, які стосуються принципових питань суспільного розвитку. Це ускладнює визначення пріоритетів державної політики з питань забезпечення національної безпеки та оцінювання її ефективності. Чинник невизначеності має набути ознак, якими можна знехтувати.

Вирішення подібних завдань має відбуватись на основі залучення нових інформаційних можливостей, серед яких особливо стрімкий розвиток демонструє ШІ. В його активі — успішне вирішення локальних завдань, побудованих на стрімких інформаційних обмінах, розробка рекомендацій щодо впорядкування соціального середовища, розширення й доповнення творчих можливостей людини тощо. На горизонті соціогенезису — поширення інтелектуальних технологій на найбільш складні суспільні сфери, до яких належить сфера національної безпеки. Суб'єктивізм та ірраціоналізм людського впливу на цю сферу повному вилученню не підлягають. Проте вони можуть бути мінімізовані на основі раціонального впорядкування інформаційних потоків, їх безперервного осмислення та розробки нових безпекових пропозицій за допомогою ШІ.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Декларація про державний суверенітет України. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text.
2. Акт проголошення незалежності України : постанова Верховної Ради Української РСР від 24.08.1991 р. URL: https://zakon.rada.gov.ua/laws/show/1427-12#Text.
3. Дашкевич Я. Питання безпеки: зміст і межі поняття. *Український час*. 1996. № 1 (15). С. 2—7.
4. Про Основні напрями зовнішньої політики України : постанова Верховної Ради України від 02.07.1993 р. URL: https://zakon.rada.gov.ua/laws/show/3360-12#Text.

5. Конституція України. URL: https://www.president.gov.ua/documents/constitution.
6. Про Концепцію (основи державної політики) національної безпеки України : постанова Верховної Ради України від 16.01.1997 р. URL: https://zakon.rada.gov.ua/laws/show/3/97-80#Text.
7. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. URL: https://zakon.rada.gov.ua/laws/show/183/98-#Text.
8. Про основи національної безпеки України : Закон України від 19.06.2003 р. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text.
9. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави : Закон України від 19.06.2003 р. URL: http://zakon3.rada.gov.ua/laws/show/975-15.
10. Про організацію оборонного планування : Закон України від 18.11.2004 р. URL: http://zakon5.rada.gov.ua/laws/show/2198-15.
11. Чорний В.С. Військова організація України: становлення та перспективи розвитку : монографія. Ніжин : Аспект-Поліграф, 2009. 368 с.
12. Степико М.Т. Українська ідентичність у глобалізованому світі : монографія. Харків: Майдан, 2020. 258 с.
13. Державна програма співробітництва України з НАТО на період до 2001 року : Указ Президента України від 04.11.1998 р. URL: https://zakon.rada.gov.ua/laws/show/1209/98#Text.
14. Про Стратегію національної безпеки України : Указ Президента України від 12.02.2007 р. URL: https://zakon.rada.gov.ua/laws/show/105/ 2007#Text.
15. Про Стратегію національної безпеки України "Україна у світі, що змінюється" : Указ Президента України від 08.06.2012 р. / URL: https://zakon.rada.gov.ua/laws/show/389/2012#n6.
16. Про Стратегію національної безпеки України : Указ Президента України від 26.05.2015 р. URL: https://zakon.rada.gov.ua/laws/show/287/ 2015#Text.
17. Про Стратегію національної безпеки України "Безпека людини — безпека країни" : Указ Президента України від 14.09.2020 р. / URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.
18. Мюнхен-2007: 15 років тому Путін почав світовий біполярний розлад. URL: https://www.ukrinform.ua/rubric-world/3401293-munhen2007-15-rokiv-tomu-putin-pocav
19. Про парламентські слухання. URL: http://www.kmu.gov.ua/control/uk/publish/article?art_id.
20. Білошицький В.І. Демократичні засади цивільно-військових відносин: зарубіжний досвід і України : дис. ... канд. політ. наук: 23.00.02. Київ, 2015. 197 с.
21. Смолянюк В.Ф. Національна безпека України: термінологічний баласт чи державотворча необхідність. *Суспільно-політичні процеси*. 2017. № 2–3. С. 76–77.
22. Пивовар М., Панько О. Особливості національної безпеки України в період воєнного стану: цілі, виклики та стратегія. *Вісник НУ "Львівська політехніка"*. Серія "Юридичні науки". 2024. № 1 (41). 266 с.
23. Про національну безпеку України : Закон України від 21.06.2018 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

24. Стратегія розвитку оборонно-промислового комплексу України від 20.08.2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text.
25. Стратегія воєнної безпеки України від 25.03.2021 р. URL: https://www.president.gov.ua/documents/1212021-37661.
26. Стратегія кібербезпеки України від 26.08.2021 р. URL: https://www.president.gov.ua/documents/4472021-40013.
27. Стратегія зовнішньополітичної діяльності України від 26.08.2021 р. URL: https://www.president.gov.ua/documents/4482021-40017.
28. Стратегія інформаційної безпеки від 28.12.2021 р. URL: https://www.president.gov.ua/documents/6852021-41069.
29. Стратегія забезпечення державної безпеки від 16.02.2022 р. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text.
30. Про основи національного спротиву / Закон України від 16.07.2021 р. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text.
31. Про утворення Ставки Верховного Головнокомандувача : Указ Президента України від 24.02.2022 р. URL: https://zakon.rada.gov.ua/laws/show/72/2022#Text.
32. Загуменна Ю.О., Сокуренко В.В. Національна безпека України в умовах воєнного стану: теоретико-правовий аналіз. *Вісник Національної академії правових наук України*. 2024. Том 31, № 2. 128 с.
33. Захист Вітчизни. URL: https://ccu.gov.ua/storinka-knygy/451-zahyst-vitchyzny.
34. Особливості застосування принципу національної безпеки в умовах воєнного стану в Україні. URL: https://ips.ligazakon.net/document/VSS01084.
35. Національна безпека України в умовах воєнного стану: загальна характеристика концепції; міжнародний аспект; нормативне регулювання; судова практика / Укладачі: Алієв Р.В., Джус О.А., Копотун І.М., Коропатнік І.М. та ін. К.: ВД "Професіонал", 2024. 480 с.
36. Пархоменко-Куцевіл О. Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти*. Серія "Екологія. Публічне управління та адміністрування". 2023. Вип. 3. 148 с.
37. Olga Reznikova, Volodymyr Smolianiuk. Konceptual Issues of National Security Policy-Making Under Uncertainty. *Vilnius University Press*. Politologia. 2023/3. Vol. 111, pp. 41–73.
38. Крутій В.О. Трансформація політичної системи суспільства в умовах гібридної війни : автореферат дис. … к. політ. н. 23.00.02. Київ : Інститут держави і права ім. В.М. Корецького НАН України, 2018. 19 с.
39. Цимбал І.В., Жовтун А.А., Ліманська О.Л. Світ VUCA як сучасний контекст інформаційних і суспільно-політичних змін. *Науковий часопис НПУ ім. М.Драгоманова*. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін. 2015. Вип. 17. С. 43–47.
40. Догадайло Я.В., Лаптєва У.Д. Передумови виживання у VUCA-світі. URL: https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/84eefdbd-cc81-4de7-a728-80cfa34781cf/content.
41. Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки і оборони. Київ, 2024. 27 с.

42. NATO Science & Technology Organization. Science & Technology Trends 2020-2040. URL: https://securitydelta.nl/media/com_hsd/ report/406/document/190422-ST-Tech-Trends-Report-2020-2040.pdf.
43. Застосування штучного інтелекту у сфері національної безпеки та обороноздатності. URL: https://sidcon.com.ua/tpost/7vuygong71-zastosuvannya-shtuchnogo-ntelektu-u-sfer.
44. Концепція розвитку штучного інтелекту в Україні : розпорядження КМУ від 02.12.2020 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.
45. Дорожня карта з регулювання штучного інтелекту в Україні. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs.

РОЗДІЛ 2
РОСІЙСЬКА АГРЕСІЯ ПРОТИ УКРАЇНИ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Сергій МОКЛЯК,
доктор політичних наук, професор

Війна в Україні прискорила глобальні процеси, зумовила зростання невизначеності, непередбачуваності та, відповідно, нервозності в поведінці окремих гравців. Це суттєво ускладнює прогнозування майбутнього, визначення стратегічних і тактичних пріоритетів, координацію поточної співпраці країн у межах спільних дій, спрямованих на подолання кризових явищ.

Глобальні трансформації, що відбуваються у світі, стосуються не тільки безпеки та протистояння ідеологій, а й формування нової економічної моделі, яка без перебільшення визначить майбутнє людства.

Світова спільнота має віднайти нову модель свого функціонування й розібратися з нинішніми політичними й економічними проблемами. Захід — як провідна цивілізація — перебуває сьогодні у кризі. Хоча ліберальним демократіям удалося розширити "велику Європу" завдяки включенню в неї постсоціалістичних держав, але цим справа й обмежилася.

Зокрема, колишній радник Президента США з питань національної безпеки Герберт Макмастер так охарактеризував ключові уроки із вторгнення росії в Україну [1].

По-перше, чергове жорстоке вторгнення в Україну в лютому 2022 року показало, що немало представників вільного світу "прикипіли" до своїх надміру оптимістичних припущень про світ після Холодної війни. Наприклад, припущення, що логіка історичного процесу нібито гарантує перевагу вільних і відкритих демократичних суспільств над закритими авторитарними системами. Західні політики вирішили, що протистояння великих світових потуг залишилося на смітнику історії. Проте голова КНР Сі Цзіньпін і президент рф В. Путін мали іншу думку. Виголошена двома диктаторами напередодні Олімпійських ігор у Пекіні спільна заява хоч і сповнена дезінформації, безкінечної підміни понять та орвеллівського перекручування правди, однак у ній було донесено чітку позицію. Вони націлилися перехопити глобальне лідерство в демократіях, які вважають розділеними, ослабленими та занепалими. Висновок із цього можна зробити такий: партнери-однодумці у всьому вільному світі мають визначити нові способи ефективного протистояння росії та Китаю.

По-друге, Захід зрозумів, що тристороння дипломатія, яку практикували Президент США Річард Ніксон і державний секретар США Генрі Кісінджер у 1970-х роках, прагнучи зробити відносини США окремо з СРСР та з Китаєм більш тісними, ніж ці дві держави мали між собою, просто неможлива у світі, де дві реваншистські потуги заприсяглися, що "дружба між двома

державами не має обмежень". Китай підтримав цю клятву, виголошену перед Олімпійськими іграми 2022 року, одіозною "дипломатією воїна-вовка", яка зумисне посилювала дезінформацію Кремля та намагалася пом'якшити фінансові й економічні збитки від упроваджених більшістю вільного світу санкцій проти рф. Ідея, щоб Китай і росія стримували одне одного, чудова, проте наші противники координують спільні дії проти вільного світу. Ці дві країни почергово відіграють ролі то "палія", то "пожежника" у конфліктах повсюди — від Сирії до Пакистану, від Північно-Східної Азії до залів засідань ООН. Тому не варто розділяти Сі й Путіна, вільний світ має розглядати двох диктаторів як єдине ціле. І не лише тому, що вони один одного варті, а й тому, що вигоди від партнерства росії та Китаю великою мірою посилюються через змогу прикривати один одного в заплутуванні, перешкоджанні, примушуванні й саботуванні.

По-третє, російська агресія та українська відвага показують, що хоча війна й не є бажаним способом розв'язання суперечок, вона буває єдиним способом зробити так, щоб хтось інший не розв'язав їх замість вас. Перефразовуючи вислів британського теолога та філософа Ґілберта Кіта Честертона, можна сказати, що потреба зміцнити колективну оборону, щоб відновити політику стримування й підготуватися до реакції на агресію, уже перезріла. США, країни НАТО та держави з-поміж їхніх однодумців, на кшталт Японії, мусять без зволікань посилити не лише свої військові спромоги, а й допомогти зміцнити оборону Тайваню з огляду на те, що можна було зробити до 24 лютого 2022 року для допомоги Україні запобігти новому російському вторгненню.

По-четверте, покладатися на авторитарні режими щодо енергоносіїв є фатальною помилкою. Для Німеччини стрибок до невідновлюваних джерел енергії в поєднанні з відмовою від ядерної енергетики став кроком у прірву "обіймів" рф. Залежність від російської нафти й газу на перших порах послабила реакцію Німеччини на чергове жорстоке вторгнення росії в Україну, змусила її спалити більше вугілля та створити більше викидів вуглецю, щоб в оселях не згасло світло. Тому можна дійти висновку, що нам потрібні нові політики, які поєднуватимуть енергетичну безпеку з національною, а також із політикою скорочення вуглецевих викидів.

По-п'яте, навіть поодинокі розриви в ланцюгах постачання, які контролюють агресори, підривають суверенітет й ускладнюють реагування на агресію. Прикладом є не тільки залежність Європи від російської нафти та газу, а й залежність Індії від російської зброї. Через це Сі Цзіньпін вибудовує економіку "подвійної циркуляції", яка, з одного боку, мало залежить від закордонних ринків, фінансів і технологій, а з іншого — посилює залежність інших держав від китайських товарів, їх базових складників і матеріалів. Наприклад, Китай намагається домінувати в ланцюгах постачання, критично важливих для переходу до чистих джерел енергії.

Таким чином, російсько-українська війна кинула тотальний виклик сучасній глобалізації світу. І нині саме Україна стала тим чинником, що визначив декілька тенденцій світового розвитку [2, 3].

По-перше, сучасний глобалізований світ перетворився на зону перманентного конфлікту між росією і Заходом. Війна консолідували країни західного світу у боротьбі з неототалітарною росією.

По-друге, Україна стала своєрідним тестом на готовність Заходу, й передусім Європи, знову знайти і виконати свою цивілізаційну місію й сформувати активну зовнішню політику, спрямовану в майбутнє. Виникає й поглиблюється розуміння причетності євроатлантичної спільноти до перемоги України. У прагненні до гідного миру нас підтримує демократичний світ, передусім євроатлантична цивілізаційна спільнота. Трансатлантична співпраця лише активізувалася після вторгнення росії в Україну. Прикметно й те, що НАТО розширилося на порозі росії: Швеція і Фінляндія відмовилися від десятиліть нейтралітету і стали повноправними членами НАТО.

По-третє, відбувається відродження і розвиток цивілізаційної суб'єктності України в євроатлантичному геополітичному просторі. Маємо визнання світом причетності народу України до євроатлантичної цивілізаційної спільноти. Україна продемонструвала готовність вийти з пострадянського стану й сірої проміжної зони та обрала європейський вектор розвитку. В дійсності ми відійшли від "руського міра", нас вже прийняли в Європу.

По-четверте, російське вторгнення в Україну продемонструвало деєвропеїзацію росії, її поворот до східного вектору своєї історії. Стан і тенденції розвитку насамперед етнодемографічної структури російського суспільства — серйозний мотив для російської еліти шукати партнерства і в мусульманському світі, і кооперуватися з Китаєм тощо.

По-п'яте, російсько-українська війна оприявнила факт неймовірної історичної ваги: усі лінії історичних протистоянь Росії з Європою пролягають культурними теренами України. Нині ми є свідками завершення російської ідеологічної парадигми, яку раніше частково перейняв і Захід: у межах цієї парадигми Україні було відведено маргінальну роль культурної провінції "руського міра". Сьогодні цікавість до України зростає з імперативною швидкістю — і на цей запит потрібно відповідати. Тому необхідно розробити й презентувати саму концепцію української культури й ролі України в європейській історії.

По-шосте, поглиблюється розуміння того, що війна росії проти України — це екзистенціальна й світоглядна війна. Війна не просто за інтереси чи потреби, а за цінності та ідентичність. І не лише для України, а й для всього західного світу. Тому реальна перемога України у війні має глобальний смисл для майбутнього людства. У нинішній російсько-українській війні крім геополітичних і економічних питань вирішується й екзистенціально-політичне питання — хто є аутентичним нащадком Київської Русі — Україна чи росія? Тому однією з причин війни росії проти України є й екзистенціальне бажання з'єднатися зі своїм корінням — Києвом як "матір'ю міст руських". Це й зумовлює позараціональний, екзистенціальний характер війни проти України. Це означає, що росія, всупереч своїм заявам, передусім воює не з колектив-

ним Заходом чи НАТО, а з усією військовою жорстокістю вирішує віковічну суперечку з Україною. Завдяки надзвичайному опору, мужності й героїзму народу Україна буквально закарбувалася на ментальній мапі багатьох людей в усьому світі — людей, які до повномасштабного вторгнення росії не знали, де є Україна на мапі світу. Тому сьогодні важливою є й проблема поширення знання про Україну за кордоном, просування українського культурного продукту та інституційні гарантії цього процесу.

По-сьоме, війна в Україні стала своєрідним каталізатором для нового гуманізму, хвилі якого розходяться по всьому світу, нейтралізуючи неототалітаризм і торуючи шлях до формування нового типу цивілізації — цивілізації подолання війни як способу вирішення конфліктів між народами, державами, країнами та союзами країн. Для цього необхідно викрити й зупинити неототалітаризм як принципово згубний шлях для людства, який заперечує демократію, права людини і, зрештою, розвиток [4].

Нинішня війна в Україні являє собою абсолютно нове явище у військовій історії. Так, Шон Макфейн відмічає, що російсько-українська війна продемонструвала не тільки нові правила війни, а й те, як воювати і перемагати проти сильніших армій у XXI столітті. Він виокремив десять правил [5]:

Правило 1. Традиційна війна відійшла в минуле.

Традиційна війна є одним із видів бойових дій — і Друга світова війна тому приклад, — але нині немає нічого більш нетрадиційного, ніж традиційна війна. З 1945 року лише 6 % війн були традиційними, а останні з них велися сорок років тому. Ніхто вже так не воює, бо це більше не дає перемоги — проте росія спробувала. У лютому 2022 року вона розпочала першу за 35 років традиційну війну і зазнала поразки. Символом її стратегічної недолугості стала 64-кілометрова російська військова колона, яка в перші тижні війни застрягла на шляху до Києва. Ведення традиційної війни потребує надзвичайного рівня дисципліни, управління й організаційної єдності, а росіяни цього позбавлені. Війна була приречена на провал, а росіяни остаточно змінили свою тактику наприкінці березня, перейшовши до російської нетрадиційної війни, яку ми бачили в Грозному й Алеппо. Це стратегія терору. Це правило пояснює, чому традиційні війни сьогодні закінчуються невдачею, і підказує, що працює краще.

Правило 2. Інвестуйте в людей, а не в технології.

Багато хто уявляє майбутню війну надзвичайно високотехнологічною, але бойовий досвід високотехнологічних збройних сил після 1945 року був жалюгідним — вони регулярно програвали низькотехнологічним арміям. Франція зазнала поразки в Алжирі та Індокитаї, Велика Британія — у Палестині й на Кіпрі, СРСР — в Афганістані, США — у В'єтнамі, Сомалі, Іраку й Афганістані, а росія, схоже, нині в Україні. Кадри скромного українського трактора, який тягне російські танки з поля бою, говорять самі за себе. Це правило пояснює, чому найкраща технологія — це 15 сантиметрів між нашими вухами. Хитрість перемагає високотехнологічну грубу силу.

Правило 3. Немає війни або миру — вони завжди співіснують.

Розумні супротивники використовують простір між війною й миром задля своєї перемоги. У 2014 році росія застосувала "зелених чоловічків", підрозділи спецназу й найманців на кшталт ПВК "Вагнер", щоб здійснити приховану окупацію на Сході України. Українці не дали себе надурити, але Захід дав. Для нього це не скидалося на традиційну війну, але й не було миром. Поки західні спецслужби все ще намагалися розібратися, що ж росія робить на Донбасі, анексія Криму стала доконаним фактом. Це правило пояснює, чому не буває війни *або* миру, а тільки війна *та* мир. Від усвідомлення цієї різниці залежить стратегія перемоги.

Правило 4. Завоювання умів і душ не працює.

Завоювання умів і душ місцевого населення не веде до перемоги, як хибно вважала більшість американських генералів в Афганістані й Іраку. І це одна з причин їхньої поразки. Упродовж В'єтнамської війни серед бійців спецназу Армії США побутувала приказка: "Якщо взяти їх за яйця, уми й душі теж будуть ваші". Таким є російський підхід до боротьби з повстанцями, і він передбачає масові вбивства цивільного населення та стирання міст із лиця землі. Саме це вони зробили з Чечнею, Сирією, а тепер і з Україною. Порушення прав людини та супутні втрати є не похибкою, а прикметою російської війни, про що свідчать Буча, Маріуполь та Ізюм. Це аморальний і огидний підхід, який використовували протягом усієї історії, нерідко успішно. Це правило пояснює, чому на війні насильство зазвичай ефективніше, ніж милосердя.

Правило 5. Найкраща зброя стріляє не кулями.

"Бій точиться тут, мені потрібна зброя, а не евакуація". Це була одна і найбільш цитованих фраз під час російського вторгнення в Україну — слова зухвалого українського Президента, який відмовився під пропозиції США залишити Київ. Справжня ця цитата чи ні — значення не має. Вона подіяла. Зброя почала надходити, і НАТО заворушилося вперше за 30 років. Україна успішно перетворила соціальні мережі й меми на зброю, легко обійшовши світового лідера з дезінформації — росію. Правило № 4 говорить нам, що уми і душі не мають значення на низовому, тобто "тактичному", рівні війни. Та на глобальному, або "стратегічному", рівні завоювання умів і душ є необхідною умовою перемоги. Український народ і влада разом ведуть успішну інформаційну війну, яка перетворила росію на державу-парію, якої цурається навіть Китай. Що ще важливіше — це дало змогу зберегти інтерес Заходу до України, що привело до збільшення кількості зброї, боєприпасів, цінних розвідувальних даних, дипломатичної та народної підтримки. Це правило пояснює, чому в інформаційну добу інформація має більшу силу, ніж летальна зброя, і як саме нею ефективно користуватися.

Правило 6. Найманці знов у грі.

Російські найманці, як-от ПВК "Вагнер", стали синонімом війни. З 2014 року ПВК "Вагнер" стала улюбленою зброєю Путіна, тому що вона дає Кремлю можливість правдоподібно заперечувати свою участь у разі про-

валу операцій, а росіяни таки провалюються. У 2018 році ПВК "Вагнер" зіткнулася із Силами спеціальних операцій США на сході Сирії та була знищена. І Москва, і Вашингтон вирішили знехтувати цим інцидентом, щоб не доводити до Третьої світової війни, ймовірність якої була б реальною, якби то були російські солдати, а не військові найманці. Найманці — друга найдавніша професія, і від них на війні великі проблеми. Це правило пояснює, у чому полягають ці проблеми, як найманці змінюють війну і як найкраще їх використовувати чи перемагати.

Правило 7. З'явилися нові типи світових сил.

Це правило не стосується України тією самою мірою, як інших збройних конфліктів у світі, наприклад нарковійн у Латинській Америці, конфліктів в Африці, релігійних війн на Близькому Сході і в Південній Азії. Національні держави всюди здають позиції, і замінює їх новий клас світових сил — супербагатії. За даними Світового банку, зі 100 найбільших генераторів прибутку у світі 71 — це корпорації і лише 29 — держави. У людському вимірі 1 % найбагатших володіє 45 % світового багатства, а бідніша половина населення планети сукупно володіє менш ніж 1 %. Тепер, коли найманці повертаються, супербагатії можуть стати озброєними й дуже небезпечними. Вони можуть розпочати війну, щоб захистити свої міжнародні інтереси, так само, як це роблять держави. Колись ExxonMobil чи Ілон Маск зможуть мати власну армію. Насправді вони *вже* можуть, якщо захочуть. Це правило пояснює, як це докорінно змінить світовий порядок.

Правило 8. Війни не завжди ведуться між державами.

Ще одне правило, яке менше стосується української боротьби, але зберігає свою важливість для решти світу. Коли супербагатії можуть набирати найманців, тоді вони можуть вести війну, неважливо, наскільки малу. Держави більше не будуть єдиними суб'єктами війни, а можуть навіть стати трофеєм. Уже сьогодні міжнародні наркокартелі воюють один з одним за вплив на вулицях Латинської Америки. Вони захоплюють країни, як-от Гватемалу, і називають їх "наркодержавами". Видобувні галузі, наприклад нафтові, газові та гірничі компанії, дедалі частіше звертаються до найманців, щоб захистити своїх людей, території та майно. Може, колись вони навіть воюватимуть одна з одною за нафтові родовища в слабких державах, які не здатні себе захистити чи мають корумпованих політиків, ласих до хабарів. Оскільки вогневу міць можна купити за гроші, супербагатії стають новим видом суперсил — а це віщує війни без держав. Це правило пояснює, якими будуть ці війни і які наслідки вони матимуть для міжнародних відносин.

Правило 9. Тіньові війни переважатимуть.

Росія захопила Крим у 2014 році засобами тіньової війни — так здавалося міжнародній спільноті, але не Україні. В інформаційну добу можливість правдоподібного заперечення є більш вирішальним фактором, ніж військова міць на полі бою. Це заганяє війну в підпілля, де вона точиться в тіні. Тіньова війна дає агресорам змогу непомітно розпалювати конфлікти, здобуваючи перемогу ще до того, як жертва зрозуміє, що її атакувало. росія,

Іран й інші довели тіньову війну до досконалості, і їхній приклад наслідують інші держави. Лівія — це одна суцільна тіньова війна: ніхто насправді не знає, хто саме перебуває на полі бою і за що воює. Тим часом Захід не розуміє природи тіньової війни, про що свідчить його млява реакція на дії росії у 2014 році. Сучасним державам, зокрема Україні, необхідно відточувати своє вміння перемагати в тіньових війнах, і це правило пояснює, як саме цього досягти.

Правило 10. Перемоги взаємозамінні.

Половина перемоги — це розуміння того, який вигляд вона має. І це правило пропонує Україні чудову стратегію для перемоги над росією сьогодні — узяти на озброєння час. Мізки важливіші за грубу силу. До питання про мізки: згадайте Троянського коня та Давида проти Голіафа. До питання про грубу силу: згадайте Першу світову війну. Є багато способів "перемогти", і більшість із них не потребуватиме величезної армії, якщо ви маєте розум. Вам потрібна стратегія, яка використовує спосіб ведення війни вашого ворога проти нього самого, подібно до того, як боєць джиу-джитсу використовує вагу свого суперника проти нього. Це правило пояснює, як вигравати в сучасних війнах.

В оборонних галузях провідних країн світу сьогодні вже чітко окреслилася тенденція розвитку, на основі принципів та функціональних якостей Четвертої промислової революції, мультиплікаторних зразків, комплексів та систем озброєння та військової техніки (ОВТ), які за своїми можливостями у рази переважають або будуть переважати існуюче озброєння (у деяких країнах — розпочалось прийняття таких ОВТ на озброєння). Такі зразки, комплекси, системи ОВТ за своїми бойовими характеристиками та наслідками від застосування будуть співставні із високоточною й навіть з ядерною зброєю. Відповідно до цього, змінюються погляди на зміст, тактику і стратегію збройної боротьби — вони розглядаються вже не як зіткнення бойових одиниць, що вражають одна одну в ході вогневого протиборства та захоплення території супротивника, а як зіткнення багатофункціональних бойових систем, основною метою якого є позбавлення конфронтуючої системи здатності до дії [6].

Створюються багатофункціональні бойові автономні та дистанційно керовані робото-технічні системи (уніфіковані платформи) із штучним інтелектом різноманітного базування та застосування в режимі реального часу для вибірково-доцільного (селективного) ураження конкретних цілей від тактичного до стратегічного рівня. З'являються принципово нові інформаційно-технічні та інформаційно-психологічні засоби інформаційної боротьби, програмно-апаратні засоби як для проведення кібероперацій, так і для захисту від них. На основі мікромініатюризації створюються малогабаритні та надмалі засоби розвідки та бойового управління тощо.

Усе це призводить до зміни взаємного впливу зброї і способів ведення бойових дій у бік усе більшої залежності останніх від технологічності та ступеню розвитку зброї. При цьому слід зрозуміти, що в основі будь-яко-

го зразка техніки, до яких відносяться і зразки ОВТ, знаходиться технологія його розроблення та виготовлення. Причому, початок "народження" новітнього зразка техніки обумовлюється появою та освоєнням нових технологічних принципів обробки сировини, що дозволяють у наступному створити потрібний зразок. Наявність базових технологій промислового виробництва технічних засобів є визначальним фактором у розвитку озброєнь [7].

Наприклад, до найбільш перспективних напрямів використання нанотехнологій, наноматеріалів і продукції на їх основі для забезпечення оборони та безпеки держави, військові вчені відносять такі:

1. Новітні конструкційні матеріали, які дозволять суттєво розширити показники надійності та експлуатаційний діапазон сучасних і перспективних зразків ОВТ;

2. Засоби зниження помітності зброї різного цільового призначення;

3. Бойове екіпірування військовослужбовців, яке суттєво підвищить захищеність, автономність та ефективність їх дій;

4. Енергетичні системи (матеріали) для озброєнь, насамперед для боєприпасів різного призначення;

5. Компактна та енергоефективна електронна компонентна база військового призначення.

Крім цього, на теперішній час активно застосовується виробництво з використанням 3D-друку у сфері оборони. Адитивне виробництво (Additive Manufacturing) (AM), добре відоме як 3D-друк, було визначено Європейською Комісією як одна з ключових технологій, що здатна підвищити конкурентоспроможність промисловості в Європі завдяки її можливостям швидкого, делокалізованого та гнучкого виробництва. AM вже використовується у цивільній промисловості та виробниками оборонного комплексу. Проте, збройні сили знаходяться ще достатньо далеко від використання потенціалу цієї технології. Технології AM — шлях до посилення оборонних можливостей. Очікуване зростання ринку AM може генерувати численні переваги для оборонної спільноти: зменшення витрат на виробництво інструментів та деталей, вдосконалення конструкції, скорочення часу на шляху до кінцевого споживача, підвищення технічної та комерційної конкурентоспроможності. Водночас 3D-друк значно вплине на обслуговування військових платформ шляхом виробництва запасних частин та компонентів обладнання. Крім того, технології AM можуть бути перспективними для посилення оборонних можливостей. Йдеться про логістичну підтримку розгорнутих сил у віддалених або ворожих середовищах. Використання цих технологій у проведенні операцій може суттєво вплинути на хід виконання місій. Час між відмовами в роботі та відновленням доступності платформ, транспортування та зберігання значної кількості запасів може зменшитись, із супутнім зменшенням витрат, скороченням логістичного навантаження на операцію.

Використання нових матеріалів для потреб оборони є також сучасним трендом. Озброєння та військова техніка стає дедалі складнішою, як і ма-

теріали, що використовуються для її створення. У цьому контексті сучасні матеріали викликають чималий інтерес, оскільки їхнє використання може суттєво вплинути на майбутню операційну ефективність військових місій. Новітні матеріали можуть застосовуватися у широкому діапазоні областей та ворожих середовищ, де ризики та пошкодження можуть бути зменшені за допомогою захисних рішень. Найбільш проривний ефект планується отримати завдяки інтеграції функціоналів різних нових розробок, таких як зберігання та застосування енергії, камуфляж, моніторинг персонального здоров'я, захист завдяки "суперінтелектуальним" матеріалам для платформ та солдатів. Інші потенційні способи використання новітніх матеріалів, які будуть вивчені в майбутньому, включають потенціал самовідновлювальних матеріалів, матеріалів кіберзахисту (реагування на електромагнітне втручання), конструкції біометричних матеріалів, морфінові аеродинамічні поверхні або інтеграція метаматеріалів.

Широкомасштабна збройна агресія російської федерації проти України засвідчила наскільки актуальним і навіть пріоритетом розвитку України стали саме військова справа та воєнна наука. У таких умовах значно зростає роль та місце воєнної науки у забезпеченні національної безпеки, яка має стати одним із основних чинників державного будівництва.

З огляду на реалії сьогодення, воєнна наука має забезпечувати упереджувальне науково-теоретичне обґрунтування актуальних проблем воєнної безпеки держави, відкривати перспективи розвитку воєнної справи та добиватися того, щоб інновації якомога швидше впроваджувались у діяльність ЗС України — їх підготовку, застосування та забезпечення.

Результати аналізу війни в Україні, який був здійснений робочою групою Генерального штабу ЗС України на чолі з генерал-майором Володимиром Ковалем, визначили низку проблем застосування частин та підрозділів ЗС України, які потребують першочергового вирішення з метою підтримання наявних спроможностей ЗС України, що дало можливість сформувати перелік пріоритетних напрямів наукових досліджень, які можливо окреслити у дванадцяти напрямках.

Напрямок 1. Сучасні технічні засоби розвідки.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

недостатня ефективність наявних засобів повітряної радіотехнічної розвідки;

Довідково. Низька точність визначення координат радіолокаційних засобів та достовірність розпізнавання типів радіолокаційних засобів. Неможливість визначення координат засобів РЕБ противника.

низька швидкість обробки розвідувальної інформації від засобів повітряної та наземної оптико-електронної розвідки;

Довідково. Недостатній рівень автоматизації процесів обробки цифрових зображень та відеопотоків.

недостатня ефективність звукометричних комплексів розвідки;

Довідково. Низька точність визначення координат об'єктів розвідки та достовірності їх розпізнавання, в тому числі ударних БпЛА та крилатих ракет. Відсутність програмно-апаратних засобів оброблення акустичних сигналів.

низька ефективність та надійність елементів наявних розвідувально-сигналізаційних систем.

Довідково. Обмежений час автономної роботи, недостатня дальність виявлення та достовірність розпізнавання об'єктів, наявність демаскуючих ознак. Відсутність технічних рішень щодо створення перешкодостійких каналів передачі даних та їх складових елементів.

Напрямок 2. Системи (засоби) автоматизованого управління, зв'язку та захисту інформації.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

неможливість автоматизованої видачі інформації з РЛС іноземного виробництва на пункти управління протиповітряної оборони та вогневі засоби;

Довідково. Невідповідність протоколів видачі інформації про повітряну обстановку РЛС іноземного виробництва з вітчизняними засобами автоматизації та вогневого ураження.

невідповідність можливостей існуючих каналів захищеного зв'язку потребам військ (сил).

Довідково. Недостатня пропускна здатність існуючих каналоутворюючих програмно-апаратних комплексів захищеного зв'язку та обміну даними.

Напрямок 3. Навігаційні та геоінформаційні системи.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є недостатня автономність та перешкодозахищеність навігаційних систем для БпЛА, роботизованих платформ наземного та морського базування.

Довідково. Зниження точності визначення координат в умовах ведення противником радіоелектронної боротьби.

Напрямок 4. Роботизовані та дистанційно-керовані системи (комплекси).

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

недостатня дальність дії та перешкодозахищеність каналів управління;

Довідково. Суттєва залежність від впливу засобів радіоелектронної боротьби та можливість компрометації каналу управління противником.

недостатній рівень автоматизації та автономності роботизованих платформ;

Довідково. Недосконалість сучасного програмного забезпечення для роботизованих та дистанційно-керованих систем (комплексів).

низька ефективність існуючих інженерних боєприпасів при використанні для створення системи інженерних загороджень;

Довідково. Відсутність малопомітних рухомих вибухових пристроїв для дистанційного ураження наземних цілей. Недостатня перешкодостійкість

каналів управління керованими мінними полями та великі габаритні розміри командно-передаючого та виконавчих пристроїв.

низька ефективність вогневого ураження стрілецькими засобами розвідувальних та розвідувально-ударних БпЛА.

Довідково. Відсутність дистанційно-керованих поворотних платформ для розміщення стрілецької зброї великого калібру та програмного забезпечення для керування ними.

Напрямок 5. Ракетно-артилерійські засоби вогневого ураження.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

недостатня ефективність ураження повітряних цілей зенітними артилерійськими засобами;

Довідково. Відсутність технічних рішень щодо розроблення зенітних артилерійських боєприпасів з програмованим підривом калібру 23 мм і більше.

недостатня оперативність нанесення вогневого ураження системами РСЗВ та артилерії в тактичній глибині бойових порядків.

Довідково. Відсутність сучасних малогабаритних мобільних систем залпового вогню з можливістю використання існуючих типів некерованих авіаційних ракет.

Напрямок 6. Зразки, системи (комплекси) озброєння.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

низька ефективність існуючих бортових засобів оповіщення про опромінювання літальних апаратів;

Довідково. Відсутність технічних рішень щодо розроблення засобів (пристроїв) для створення бортових систем оповіщення про опромінювання літального апарату.

недосконалість вітчизняних та висока вартість закордонних зразків бойового екіпірування.

Довідково. Відсутність технічних рішень щодо створення окремих елементів комплексів бойового екіпірування.

Напрямок 7. Системи РЕБ, кіберборотьби та протидії технічних розвідкам.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є низька ефективність засобів протидії високоточній зброї противника.

Довідково. Відсутність технічних рішень для одночасного подавлення існуючих систем навігації оперативних, оперативно-тактичних, ударних БпЛА та крилатих ракет.

Недостатні можливості щодо постановки перешкод бортовим радіовисотомірам крилатих ракет.

Напрямок 8. Системи (засоби) захисту та безпеки військ.

Проблематикою ЗС України, що потребує першочергового вирішення за цим напрямком є:

невідповідність технічних характеристик сумішей для засобів аерозольного прикриття можливостям сучасних засобів оптико-електронної розвідки та наведення засобів високоточної зброї;

Довідково. Відсутність сумішей для аерозольного прикриття об'єктів, військ (сил) від тепловізійних засобів розвідки та протидії системам наведення високоточних засобів ураження в діапазоні довжин хвиль (8…14) мкм.

недостатні ергономічні показники наявного екіпірування військовослужбовців;

Довідково. Відсутність сучасних матеріалів та технологій створення засобів індивідуального захисту.

недостатня ефективність і висока вартість наявних засобів маскування та введення в оману;

Довідково. Відсутність сучасних технологій розроблення засобів маскування та введення в оману.

недостатній рівень інженерного захисту об'єктів критичної інфраструктури від ударів з повітря;

Довідково. Відсутність засобів і технологій інженерного захисту об'єктів критичної інфраструктури.

недостатні спроможності та низька ефективність розмінування місцевості.

Довідково. Мала відстань подачі заряду розмінування та недостатня точність укладки заряду розмінування на мінному полі. Мала вибухостійкість тралів бойових машин розмінування та висока небезпека для особового складу екіпажу.

Напрямок 9. Зразки озброєння на нових принципах дії.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є відсутність зразків озброєння на нових принципах дії для підвищення ефективності ураження об'єктів противника.

Довідково. Відсутність вітчизняних технологій створення лазерних, електромагнітних та кінетичних засобів ураження.

Напрямок 10. Зразки технічних засобів логістичного забезпечення та життєдіяльності.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

недостатня якість засобів забезпечення життєдіяльності військ (сил) в польових умовах;

Довідково. Низька мобільність, великі масо-габаритні розміри, недостатня захищеність споруд для розміщення особового складу та матеріально-технічних засобів для забезпечення життєдіяльності військ (сил).

потреба зниження маси при збереженні потрібної калорійності пайків для підрозділів, що ведуть автономні бойові дії або виконують спеціальні завдання.

Довідково. Відсутність сублімованих пайків вітчизняного виробництва для забезпечення автономності дій тактичних груп (малих підрозділів).

Напрямок 11. Безпілотні літальні апарати.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

низька ефективність пошуку малорозмірних замаскованих цілей бортовими оптико-електронним засобами;

Довідково. Відсутність багатоспектральних (гіперспектральних) бортових оптико-електронні засобів з технологією штучного інтелекту.

низька перешкодозахищеність каналів керування та передачі даних БпЛА;

Довідково. Недосконалість технології створення перешкодозахищених каналів керування та передачі даних БпЛА.

низька ефективність пошуку підводних об'єктів з використанням існуючих засобів;

Довідково. Відсутність магнітометричної розвідки, які можуть застосовуватися на БпЛА. Відсутність технологій створення малогабаритних засобів гідроакустичної розвідки, які можуть застосовуватися на БпЛА.

обмежені можливості наведення ударних БпЛА на активні джерела радіовипромінювання (станції РЕБ, оглядові РЛС та РЛС ЗРК).

Довідково. Відсутність технологій створення бортових систем виявлення та наведення БпЛА на активні джерела радіовипромінювання (станції РЕБ, оглядові РЛС та РЛС ЗРК).

Напрямок 12. Технології та засоби медичного забезпечення.

Проблемою ЗС України, що потребує першочергового вирішення за цим напрямком є:

низькі можливості індивідуального та колективного контролю за фізичним станом для своєчасного відновлення функцій та реабілітації військовослужбовців;

Довідково. Відсутні засоби та матеріали контролю фізичного стану, відновлення функцій та реабілітації військовослужбовців.

недостатня своєчасність та ефективність надання домедичної допомоги на полі бою;

Довідково. Недосконалість існуючих засобів та способів надання домедичної допомоги.

недостатня якість і висока вартість протезування та забезпечення відновлення основних життєво-важливих функцій людини, що зазнала поранень.

Довідково. Відсутність вітчизняного виробництва роботизованих механічних протезів кінцівок з електронними імплантатами управління рухом.

Цей перелік, звісно, не є вичерпним. У ньому виокремлено головні тенденції, які сучасна воєнна наука зобов'язана вирішувати. Зрозуміло, що дати точний прогноз, якими будуть війни майбутнього, складно, але осягнути характер змін воєнних конфліктів, запропонувати шляхи розвитку ЗС України є головним і цілком реалістичним завданням воєнної науки.

Іншим важливим, але більш практичним, завданням воєнної науки є розробка нових форм застосування ЗС України, які сьогодні перебувають у застарілій парадигмі. Розвиток засобів збройної боротьби обумовлює перехід

від фізичного знищення противника тільки вогневими засобами до комплексного впливу, у п'ятьох доменах ведення збройної боротьби, що відповідає середовищам (суходіл, повітря, море, космос, кіберсередовище), а також трьом просторам (фізичному, кібернетичному та інформаційному).

Вбачаються такі пріоритетні напрями переозброєння ЗС України:

1. Розробка власних ракетних комплексів, зокрема великої дальності, з метою створення сил стримування.

2. Розробка систем протиракетної оборони, зокрема для боротьби з гіперзвуковими ракетами.

3. Розробка ракетних систем повітряного базування із збільшеною дальністю виявлення та ураження цілей.

4. Розробка новітніх систем протиповітряної оборони, зокрема з БпАК.

5. Розробка новітніх засобів радіоелектронної розвідки та радіоелектронної боротьби.

6. Збільшення дальності вогневого ураження артилерійських систем.

7. Підвищення мобільності військ.

8. Завершення створення автоматизованих систем управління як єдиної системи ураження, розвідки, радіоелектронної боротьби, інформаційного протиборства.

9. Впровадження наукових рішень для проведення операцій в кіберпросторі.

Організаційна структура української оборонної промисловості та система управління нею є недієвою і малоефективною, внаслідок чого поступово зменшується інноваційна складова діяльності, результативність та ефективність також мають сталу тенденцію до зменшення, зокрема:

у виробництві переважають технології третього і четвертого технологічних укладів, не створено належних набутків п'ятого і шостого технологічних укладів, що призводить до невідповідності лінійки систем, підсистем озброєння та військової техніки, що виробляються підприємствами, сучасному рівню;

темпи переозброєння Збройних Сил України, інших складових сил оборони на новітні (модернізовані) зразки не забезпечують завантаженість виробництва в оборонній промисловості і, як наслідок, підприємства мають обмежені можливості для інвестицій у ліквідацію технологічного відставання, існування та розвиток підприємств можливі лише у разі наявності портфеля іноземних замовлень;

через російську військову агресію та тимчасову окупацію частини суверенної території України були втрачені підприємства оборонно-промислового комплексу, які виробляли озброєння, військову та спеціальну техніку та/або брали участь в кооперацийних зв'язках з іншими підприємствами — виробниками озброєння, військової та спеціальної техніки тощо [8].

Все це відіграє суттєву роль у формуванні платформи розвитку оборонно-промислового комплексу (ОПК) України.

В умовах широкомасштабного вторгнення з боку російської федерації особливого значення для України набуває загальна проблема досягнення

балансу: з одного боку, забезпечення обороноздатності країни завдяки впровадження інноваційних рішень та наукових досліджень ЗС України в розвиток критичних технологій, з іншого боку, обґрунтування витрат на потреби оборони та розвиток підприємств ОПК.

Військовий конфлікт в Україні став потужним стресом для її економіки, оскільки низка галузей, пов'язаних зі споживчим ринком, зазнала суттєвих втрат. У цих умовах відновлення воєнного потенціалу України може сприяти зростанню її економіки завдяки зміцненню ОПК, розвитку виробництва товарів подвійного використання, а також галузей, орієнтованих на обслуговування армії [9].

Для подолання залежності оборонної промисловості України від імпорту товарів іноземного виробництва виникла вкрай необхідна потреба у заохоченні населення країни та науково-технічного потенціалу ЗС України у направленні власних інноваційних рішень та наукових досліджень на розвиток оборонної галузі. Крім того, невід'ємною умовою забезпечення інноваційного розвитку оборонної промисловості України є також налагодження тісної співпраці між виробниками військової продукції, її замовниками та науковими організаціями. Одним зі шляхів залучення додаткових фінансових ресурсів та збільшення інвестиційної привабливості підприємств ОПК України є створення технологічних парків в оборонній галузі. Основною метою такої форми об'єднання, перш за все науково-виробничого потенціалу держави, є забезпечення швидкої реалізації інноваційних наукових розробок.

З огляду на вищевказане, зрозуміло, що впровадження інноваційної діяльності у поєднанні з науковими дослідженнями у сферу оборонно-промислового комплексу — це задоволення потреб держави в сучасних високоефективних системах озброєнь, військовій та спеціальній техніці відповідно до встановлених нормативів, національних та міжнародних стандартів, а також потреб експорту наукоємної продукції шляхом оновлення та формування нової науково-технологічної бази підприємств та організацій ОПК за допомогою поєднання ефективного державного управління і ринкових механізмів саморозвитку.

Інноваційна діяльність у сукупності із науковими дослідженнями та необхідні заходи щодо їх розвитку мають розглядатися з урахуванням таких основних пріоритетів:

адаптація інноваційної інфраструктури у сфері ОПК до умов глобалізації та підвищення її конкурентоспроможності;

створення привабливих умов для творців інновацій, стимулювання інноваційної (наукової) активності підприємств ОПК;

переорієнтація інноваційної інфраструктури на ринковий попит і споживача;

системний підхід в управлінні інноваційною діяльністю, інформаційне забезпечення.

Основними шляхами інноваційного розвитку ОПК України є такі:

реформування інституційного складу ОПК з утворенням науково-виробничих структур, здатних реалізувати повні інноваційно-інвестиційні цикли;

створення нової системи управління функціонуванням і розвитком ОПК;

застосування системи прискореного інноваційного розвитку та нової моделі наукового забезпечення інноваційної діяльності у сфері ОПК;

введення в дію нових механізмів фінансування, кредитування та інвестиційного забезпечення оборонно-промислового комплексу;

надання науково-виробничим структурам ОПК державної підтримки на внутрішньому та зовнішньому ринках.

Заходи з реформування ОПК для активізації інноваційної діяльності мають ґрунтуватися на результатах наукових досліджень з аналізу та прогнозування:

соціально-економічного стану в сфері оборонно-промислового комплексу України на 5, 10, 15 років з оцінюванням можливих обсягів фінансування ОПК;

попиту та цін на продукцію військового та подвійного призначення;

цін на головні типи ресурсів, які використовуються під час виробництва продукції військового і подвійного призначення;

технологій, які використовуються під час виробництва продукції військового і подвійного призначення;

наявних можливостей України з виробництва продукції військового і подвійного призначення;

можливих сценаріїв розвитку військово-політичної, технологічної, ресурсної ситуації у світі і в Україні;

можливих ризиків.

Очевидно, що без нової генерації кадрів з високим рівнем підготовки неможливо забезпечити інноваційний розвиток оборонної промисловості України. Потрібні спеціалісти у сфері розробки та реалізації високих технологій, які можуть комплексно поєднувати дослідницьку, проєктну і підприємницьку діяльність, спрямовану на організацію високоефективних виробничих структур і здатні створювати конкурентоспроможну продукцію.

Відновлення втраченого та відтворення нового оборонного потенціалу України сприятимуть розвитку сучасних технологій. Розвиток українського ОПК, оновлення його технологічної бази неможливі без розвитку інноваційної діяльності та наукових досліджень держави.

Новації у XXI столітті нерозривно пов’язані із ерою Інтернету, штучного інтелекту, біотехнологіями, пошуком альтернативних джерел енергії. Військові дії в Україні мають суттєвий вплив на інноваційне середовище країни. Це обумовлено низкою факторів, зокрема війна призвела до суттєвих економічних викликів: до зниження рівня інвестицій, збільшення ризику для бізнесу та зниження внутрішнього попиту на продукцію. Ці фактори стали перешкодою для розвитку інноваційного середовища країни; велика кількість технічних експертів та інноваційних підприємців залишили країну під час конфлікту. Це призвело до втрати технічної експертизи та зменшен-

ня кількості інноваційних проєктів; неспровокований конфлікт та економічні складнощі знизили доступність фінансування для інноваційних проектів в Україні. Більшість фінансових ресурсів сконцентрована у секторах, які потребують великих капіталовкладень, таких як будівництво та енергетика. У глобальному рейтингу інновацій *[10]* Україна із 49 місця, у 2021 р., перемістилась на 57 позицію, у 2022 р.

Незважаючи на ці виклики, українські інноваційні підприємства та стартапи продовжують розвиватися. Країна продовжує залучати іноземні інвестиції та удосконалювати інноваційні програми та інфраструктуру. Деякі інноваційні проєкти були спрямовані на вирішення проблем, пов'язаних з війною та її наслідками, такі як проєкти з відновлення та будівництва інфраструктури. Ще у довоєнний період Україна мала низку інноваційних ініціатив, спрямованих на розвиток інноваційного сектору, підтримку стартапів та інших інноваційних проєктів. Деякі з цих ініціатив включають: "Дія" — програма розвитку економіки та інновацій, яка започаткована в Україні в 2020 році. Її мета полягає в спрощенні бізнес-процесів, зниженні адміністративного навантаження на бізнес, залученні інвестицій та стимулюванні експорту; програма "Startup Ukraine" має на меті підтримку стартапів та розвиток інноваційних компаній в Україні шляхом надання фінансової та інфраструктурної підтримки; програма "Prozorro", що започаткована у 2014 році, і вона має на меті забезпечення прозорості та ефективності закупівель в Україні. Програма функціонує на відкритій платформі для проведення електронних торгів, що дозволяє зменшити корупцію та підвищити ефективність закупівель.

Міністерство цифрової трансформації, Міністерство оборони, Генеральний штаб Збройних Сил України, Рада національної безпеки і оборони, Міністерство з питань стратегічних галузей промисловості, Міністерство економіки заснували єдину координаційну платформу в галузі defense tech в Україні Brave1. Представники державних інституцій підписали меморандум про взаємодію та підтримку в рамках проєкту, метою якого є поставка на озброєння та передача для фронту передових українських технологічних рішень для переваги над ворогом і перемоги, комплексна підтримка українських розробників у галузі інноваційних оборонних технологій та розвиток сфери задля перетворення України в світового лідера defense tech.

Війна активізувала сотні українських компаній в галузі defense tech, які розробляють сучасні рішення для ведення "розумної війни". Україна вразила світ винахідливістю, швидкими нетривіальними рішеннями та ефективним застосуванням проривних технологій. Ці рішення посилюють оборонну здатність країни, зберігають життя захисників та цивільних і ефективно використовують ресурси завдяки технологічним інноваціям: дрони, роботизовані системи, центри ситуаційної обізнаності, штучний інтелект, кібербезпека, системи зв'язку, супутникові дані та багато іншого. Інноваційні розробки для армії швидко випробовуються та перевіряються в умовах бойових дій, вдосконалюючись у відповідності до задач і цілей сил безпеки і оборони.

Саме для прискорення впровадження таких розробок було створено Brave1 як єдине вікно співпраці defense tech компаній, держави та військових, а також інвесторів, волонтерських фондів, медіа і усіх хто допомагає наближати перемогу через технології.

Фокус діяльності Brave1 зосереджений на 5 напрямках:

1. *Invest:* надавати гранти розробникам, що визначені пріоритетними для потреб сил безпеки та оборони;

2. *Invent:* допомагати силам безпеки і оборони знаходити ефективні технологічні рішення в середовищі українських розробників;

3. *Platform:* створити платформу, що об'єднує усіх стейкхолдерів галузі;

4. *Showcase:* забезпечення взаємодії з силами оборони через демонстрацію їм розробок та отримання зворотного зв'язку щодо їх використання;

5. *Boost:* надати всебічну підтримку проектам, визначеним пріоритетними для сил безпеки і оборони.

Всебічна взаємодія державних і приватних стейкхолдерів в рамках Brave1 та підтримка галузі не лише допоможе армії вже сьогодні, а й стане потенціалом для масштабування українських defense tech рішень у світі, що пройшли апробацію і довели ефективність у найзапекліших боях.

Досвід європейських країн показав високий потенціал використання технологічних платформ (ТП). Тому на черговому етапі концентрації фінансових і організаційних ресурсів на найважливіших напрямах науково-технічного розвитку український уряд зміг покласти в основу науково-технічної політики саме концепцію формування ТП. Хоча для України практика створення ТП є відносно новою, проте наша країна активно просуває використання цього інструменту для забезпечення інноваційного розвитку економіки. Одним із ключових умов успіху ТП було названо участь органів влади і для України ця умова також є досить важливою. Відзначено, що учасники європейських майданчиків далеко не однаково активні. Зазвичай лідерами є великі компанії, а малі та середні фірми найчастіше розглядають даний інструмент як спосіб залишатися в курсі останніх тенденцій розвитку. Така "нерівність", природно, відчувається і в Україні. В Україні створення ТП перебуває на початковому етапі і не набуло масового характеру. Так, для України ТП — це принципово новий і досить складний для практичної реалізації інструмент. Важко прогнозувати результати від створення і функціонування даних структур в Україні, оскільки не існує чіткого правового документа, який би регулював діяльність цього механізму в нашій країні. Попри це, в Україні вже сформувалися передумови, які вимагають формування ТП як оптимального механізму подальшого науково-інноваційного розвитку. Такими передумовами є [11]:

наявність стратегічних технологічних викликів;

необхідність представлення різних груп інтересів під час розв'язання питань технологічної модернізації економіки та вибору форм партнерства бізнесу, науки, держави;

слабка спрямованість підготовки кадрів на забезпечення потреб технологічного розвитку економіки; необхідність узгодження інтересів і визначення вимог до найважливіших базових технологій;

скорочення термінів визначення актуальних пріоритетів у проведенні досліджень і розробок, напрямів технологічної модернізації та консолідації ресурсів суттєвої частини бізнесу на реалізацію таких пріоритетів для забезпечення лідерства;

необхідність вдосконалення галузевого регулювання окремих ринків продукції для підвищення інноваційної активності компаній, поширення передових технологій, залучення стратегічних інвестицій;

потреба в суттєвому поліпшенні наявних механізмів фінансової підтримки науково-технічних, інноваційних, інвестиційних проєктів;

недостатній вплив бізнесу на визначення тематики досліджень та розробок, які підтримуються державою, на систему підготовки та перепідготовки кадрів з урахуванням реально затребуваних на ринках компетенцій технологічного розвитку секторів економіки;

потенційне багатогалузеве застосування технологій;

необхідність взаємодії компаній із різних секторів для досягнення результативності технологічного оновлення; багатогалузевість досліджень для розроблення перспективних технологій;

недостатньо розвинені механізми прямої взаємодії компаній з науковими та освітніми організаціями.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Макмастер Г. Поля битв. Боротьба за захист вільного світу. Київ : Наш формат, 2023. 424 с.
2. Смолій В. А., Ясь О. В. Сучасна російсько-українська війна у світлі постколоніалізму. *Вісник НАН України*. 2022. №6 (36). С. 3–16.
3. Козловець М. А. Світовий порядок XXI століття: вектори трансформації : матеріали XXXV Харківських політологічних читань. м. Харків, 28 квітня 2023 р. Харків : Право, 2023. С. 20–25.
4. Пирожков С. І., Хамітов Н. В. Війна і мир в Україні: шляхи до реальної перемоги і розвитку. *Вісник НАН України*. 2022. №9 (39). С. 38–49.
5. Макфейн Ш. Нові правила війни. Перемога в епоху хаосу / пер. з англ. Ігор Бігун. Київ : Наш Формат, 2023. 256 с.
6. Теоретичні засади управління оборонними ресурсами: монографія. / [В.В.Коваль, О.М. Семененко, Л.В. Скуріневська, С.П. Мокляк, І.М. Ткач, С.В. Ясенко]; під ред. О.М. Семененка. Київ : Генеральний штаб Збройних Сил України, 2023. 485 с.
7. 10 трендів майбутнього, які армія України поки що ігнорує. URL: https://defence-ua.com/minds_%20and_ideas/10_trendiv_majbutnogo-2067 (дата звернення: 24.01.2025).

8. Про рішення Ради національної безпеки і оборони України від 18 червня 2021 року “Про Стратегію розвитку оборонно-промислового комплексу України” : Указ Президента України № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text (дата звернення: 24.01.2025).
9. Реформування та розвиток підприємств оборонної галузі в контексті посилення економічного потенціалу України / В. Бегема, В. Шемаєв, П. Толок // Причорноморські економічні студії. 2017. №23. С.32–36
10. Global innovation index 2023 : Global innovation index. 2023. URL: https://www.wipo.int/en/web/global-innovation-index (дата звернення: 24.01.2025).
11. Концепція формування технологічних платформ в Україні : Європейські технологічні платформи та створення платформ в Україні. 2020. URL:https://old.nas.gov.ua/siaz//Ways_of_development_of_Ukrainian_science/article/12076.2.011.pdf (дата звернення: 24.01.2025).

РОЗДІЛ 3

ШТУЧНИЙ ІНТЕЛЕКТ У КОНТЕКСТІ ДЕМОКРАТИЧНИХ І АВТОРИТАРНИХ БЕЗПЕКОВИХ ПРАКТИК

Марія КАРМАЗІНА,
доктор політичних наук, професор

3.1. Глобальна гонка за ШІ: аналіз акцентів сучасного англомовного наукового дискурсу

Штучний інтелект — блискуча технологія, стрімкий розвиток якої (поруч із досягненнями в робототехніці, блокчейнах і віртуальній реальності) у першій чверті XXI століття (як свідчить аналіз наукового дискурсу) зумовив, формування, щонайменше, трьох тенденцій у її сприйнятті. Перша з них пов'язана з тим, що в одних сучасників (тих, які слідом за Д. Безосом повірили, що "ми — на початку золотого віку ШІ" [1]) штучний інтелект породив надію на збільшення ефективності "людини з ШІ", як і "країни з ШІ". Ця обставина (упродовж, приблизно, півтора десятиліття), як і те, що за останні пару років — з моменту запуску *ChatGPT*, який засвідчив трансформацію ШІ, і його перетворення з нішевої технології на технологію, що зазнала масового впровадження, докорінно змінивши спосіб/можливість доступу до інформації та взаємодії з нею, — сформувала в середовищі інноваційних лідерів підґрунтя для своєрідної глобальної "гонки за ШІ". Остання розпочалася не лише між США як батьківщиною ШІ, та ЄС і КНР (про що свідчить, зокрема, розвиток американських технологічних гігантів *OpenAI*, *Google*, *Microsoft* і *NVIDIA*, китайських *Baidu*, *Alibaba* та *Tencent*): нині до гонки успішно долучилися Південна Корея, Індія та Японія. Для інших же умів і душ, сконцентрованих, передовсім, на нинішніх, як і потенційних загрозах і ризиках (унікальних ризиках, названих "Привидом Кіссінджера", оскільки саме Г. Кіссінджер, зауваживши настання непередбачуваної революції в нашій свідомості та мисленні під впливом ШІ, наголосив і на неминучій еволюції в нашому розумінні істини та реальності [2]), пов'язаних із ШІ, новітня технологія стала тригером неспокою, непереборних страхів, а часом і відчаю у передчутті технологічної сингулярності, про що, наприклад, у листопаді 2023 р. писав *The Economist* [3], оповідаючи про звільнення Сема Альтмана з *OpenAI* та розкол у світі технологій між "думерами" та "бумерами", перші з яких перебувають під впливом "ефективного альтруїзму", будучи стурбовані можливістю ШІ в перспективі знищити людство, а другі — "применшують страх перед апокаліпсисом штучного інтелекту". А наприкінці січня нинішнього року до кола збентежених долучився і Ватикан, оприлюднивши Заувагу "Antiqua et nova" [4], в якій представив погляд на виклики і можливості, пов'язані із розвитком ШІ у таких сферах, як сфе-

ра освіти, економіки, охорони здоров'я, стосунків і військових дій, наголосивши, що потенціал ШІ може посилити військові ресурси і вивести "далеко за межі людського контролю", прискорюючи "дестабілізуючу гонку озброєнь з руйнівними наслідками для прав людини".

Зрештою, є й ті, які відчули нездоланний скепсис щодо майбутнього ШІ, вбачаючи в ньому новітню "технологічну бульбашку", яка швидко вичерпає свій потенціал. Тож, якщо про 2023 рік медіа писали як про рік, коли ШІ став мейнстрімом [5], то уже у 2024 р. зауважували, що "блиск штучного інтелекту почав зникати", передовсім, тому що "прогрес уповільнився" [6].

Оминувши увагою точку зору скептиків, ретельніше проаналізуємо перші дві позиції. У ході цього аналізу очевидним стає те, що, осмислюючи позитив у використанні і розвитку ШІ, його адепти звертають увагу, найперше, на те, що результатом співпраці людини і генеративного ШІ (як зазначив професор Вортонівської школи бізнесу Ітан Моллік у своєму "миттєвому бестселері" 2024 р. "Спільний інтелект: життя та робота з ШІ" [7]) стає синергія, яка перевершує індивідуальні зусилля будь-якої особистості. Тобто ШІ стає не просто інструментом для підвищення продуктивності особи на робочому місці (допомагає планувати та чітко окреслювати пріоритети, здійснювати менеджмент електронної пошти та загалом звільняти особистість від рутини) — симбіоз людини та ШІ все більше виявляється чинником, що уможливлює інновації та подальший прогрес. При цьому для людини зростає комфортність взаємодії зі ШІ, оскільки останній (зокрема такі помічники, як *Google Assistant*, *Alexa*, *Siri*) налаштований як компаньйон — на персоналізовану взаємодію — і здатен не лише розуміти емоційний стан користувача (за виразом обличчя, тембром голосу, швидкістю друку) чи шляхом запам'ятовування його вподобання та поведінки, але й інтегрувати зроблені ним візуальні, голосові чи текстові введення, і, як наслідок, ШІ виявляється спроможним чітко виконувати рутинні завдання, змінювати свої рекомендації для користувача, уникаючи ситуацій, які могли б призвести його до розчарувань та, відповідно, зумовили зниження його ефективності в низці процесів.

Зосереджуючись на найвагоміших досягненнях ШІ та потенційних його можливостях, дослідники виділяють, щонайменше, півтора десятка переваг, які неодмінно зумовлять подальший розвиток ШІ в інтересах людини. Так, приміром, осмислюючи тенденції у розвитку ШІ, *Techstartups* виокремив [8] низку однозначно домінантних серед них та зауважив, що:

вертикальні агенти ШІ (спеціалізовані інструменти, призначені для автоматизації всіх робочих процесів) уже здатні замінити *SaaS* — програмне забезпечення (ПЗ) як послугу, що розвивалося з початку 2000-х і яке по-своєму переосмислило спосіб доступу компаній до ПЗ та його використання, змінивши громіздкі локальні установки масштабованими хмарними рішеннями та розблокувавши ринок у 300 мільярдів доларів: вертикальні агенти ШІ не просто роблять робочі процеси ефективнішими, але революціонізують їх, виявляючи спроможність замінити цілі команди та функції на

підприємствах, сприяючи самостійному виконанню завдань користувачами [8]. Агентний ШІ, хоч і перебуває на ранніх стадіях розвитку, але вже може виконувати завдання, які, як вважалося, вимагали людського судження (наприклад, щодо планування зустрічей, складання звітів або керування ланцюгами поставок, написання коду чи бронювання подорожей, взаємодії з клієнтами, зменшуючи витрати та підвищуючи рівень задоволеності). Серед найновіших даних розвитку ШІ у цьому напрямку — зусилля створеного після обрання Президентом США Дональда Трампа Департаменту ефективності уряду (DOGE) на чолі з Ілоном Маском, спрямовані на створення спеціального індивідуального чат-бота *GSAi* (зі ШІ) для загальних служб Адміністрації Д. Трампа з метою підвищення повсякденної продуктивності близько 12 тис. співробітників, зосереджених на керуванні офісними будівлями, контрактами та ІТ-інфраструктурою у федеральному уряді [9];

мультимодальний ШІ виявляє здатність інтерпретувати та реагувати, аналізуючи текст, зображення, аудіо та відео. Відтак — стає віртуальним помічником (на зразок *ALexa*), здатним створювати презентації, редагувати мадіафайли, діагностувати (наприклад, проблеми авто в ході вивчення фотографій чи звукозаписів) чи допомагати аналізувати дані (наприклад, лікарям в аналізі спектру даних у різних форматах);

ШІ з відкритим вихідним кодом кидає виклик не лише пропрієтарним системам (ПЗ, на яке зберігаються майнові чи немайнові авторські права), але й, як, наприклад, найновіша безкоштовна китайська модель ШІ *Deepseek*, що з'явилася наприкінці 2024 р., розширює межі доступності та продуктивності, змінюючи/вирівнюючи умови гри та даючи можливість невеликим компаніям і стартапам створювати конкурентоспроможні інструменти зі ШІ, не вимагаючи значних бюджетів; крім того — стимулювати інновації, сприяти співпраці та встановлювати нові стандарти прозорості та продуктивності, кидаючи виклики домінуванню *OpenAI* і *Google*, які інвестують значні кошти в закриті системи, заради збереження конкурентоспроможності [8]. Це "змінює ландшафт штучного інтелекту, викликаючи дебати щодо доступності, інтелектуальної власності та довгострокової стійкості в цій галузі";

генеративний ШІ уже не обмежується текстом: такі інструменти візуалізації вмісту, як *DALI-E*, революціонізують створення реклами, удосконалюють оповідь за допомогою фотореалістичних зображень. У музиці та аудіо ШІ створює персоналізовані треки (для маркетингових кампаній або розваг). У науці і медицині такі платформи, як, наприклад, *AlphaFold*, скорочують час, необхідний для відкриття нових ліків або матеріалів;

спеціалізовані моделі AI Step Up все більше задовольняють потреби в конкретних галузях: виявляють фінансове шахрайство **(**аналізуючи моделі транзакцій з високою точністю), діагностують захворювання або прогнозують результати (щодо стану пацієнтів за допомогою спеціальних наборів даних), виконують все складніші завдання із більшою ефективністю (наприклад, у сфері логістики). При цьому спеціалізований ШІ потребує менше обчислювальних потужностей та оптимізований для середовища з об-

меженими ресурсами, що робить їх ідеальними для периферійних пристроїв (дронів, датчиків *IoT* чи автономних транспортних засобів), де обробка даних у реальному часі є критично важливою.

Крім того, аналізуючи можливості та переваги ШІ у майбутньому науковому пошуку, *Techstartups* відзначив [8], що, ШІ вже обробляє величезні обсяги даних і виявляє закономірності, які люди можуть не помітити та пропустити. ШІ уже показав результати не лише у відкритті нових ліків, чи виявленні нових методів лікування (за місяці, а не за роки), але й сприяв розвитку персоналізованої медицини (використовуючи аналіз генетичних даних у ході терапії для окремих пацієнтів, або, як зауважила професорка Фей-Фей Лі у своїй книзі "Світи, які я бачу: цікавість, дослідження та відкриття на зорі ШІ" [10], що побачила світ у 2023 р.), уможливлюючи, приміром, моделювання тривимірних середовищ — тренажерів для точної візуалізації анатомії пацієнтів); у сфері матеріалознавства ШІ довів спроможність розробляти "стійкі альтернативи" пластмасам та надміцні матеріали для таких галузей, як будівництво та авіакосмічна промисловість; у математиці алгоритми здатні вирішувати "давні проблеми": віднаходять докази для складних теорем, оптимізують проєкти мереж, відкривають нові кордони в технологіях та інженерії. І все це докорінно змінює перспективи подальших наукових досліджень.

У сфері освіти ШІ допомагає викладачу персоналізувати навчальний процес, адаптуючи плани і темпи проходження уроків до потреб окремого учня чи студента. Надалі ж ШІ, як прогнозують, сприятиме виявленню та усвідомленню надавачем освітніх послуг інформації щодо прогресу учнів у режимі реального часу та допомагатиме у розробці більш ефективних стратегій навчання.

Такі інструменти, як *Adobe Firefly* та *DALL-E*, стають у нагоді фахівцям (зокрема маркетологам, художникам, дизайнерам тощо) у творчій індустрії, генеруючи ідеї, варіації вмісту, пропонуючи оригінальні концепції творів та забезпечуючи їх персоналізацію.

Підтримуючи бізнес, ШІ змінює спосіб прийняття рішень, адже розробляються інструменти, які можуть прогнозувати поведінку клієнтів: зокрема, аналізуючи масивні набори даних, ШІ створює ультрацільові маркетингові кампанії. ШІ оптимізує комерційні операції, коригуючи, наприклад, ланцюги постачання в реальному часі та забезпечуючи гнучкість бізнесу. ШІ скорочує терміни розробки продукту, проєктуючи, тестуючи, ітеруючи все швидше і швидше.

В інженерії можливості ШІ розширюватимуться для проведення структурного аналізу, моделювання чи створення прототипів, а також для тестування більш складних систем, прискорення розробки продукту та покращення заходів безпеки [8].

Іншою особливістю розвитку ШІ є те, що цей процес активізує як дискусії щодо етики та нормативних рамок його застосування, пов'язані із вирішенням проблем конфіденційності (захисту даних користувача)

чи авторського права, уникненням упередженості алгоритмів (як результату навчання на даних певного типу) і підзвітності у контексті глобального співробітництва, так і акцентує відмінності у пріоритетах держав та урядів, пов'язаних із бажанням технологічного домінування (найперше, у сфері безпеки, оборони, розвідки) і забезпечення національної стійкості. Остання має забезпечуватися використанням ШІ в екологічних практиках, в оптимізації енергетичних систем (прогнозуванні попиту, балансуванні постачання, інтеграції відновлювальних джерел), у сільському господарстві (використання інструментів для "точного землеробства" та масштабування практик сталого землеробства), "зелених технологіях" (для забезпечення постійного доступу до енергії з відновлюваних джерел, зокрема — у періоди низької генерації), у галузі "циклічної економіки", як і в моделюванні та прогнозуванні клімату чи в прогнозуванні ланцюга поставок.

Забезпечення проривів ШІ, на думку експертів, відбувається/відбуватиметься не тільки завдяки удосконалення алгоритмів чи ПЗ, але й завдяки процесорам нового покоління (на чому зосереджені виробники мікросхем *AMD, Intel, NVIDIA*), апаратним інноваціям (прискорювачам ШІ на зразок модулів обробки тензорів *Google (TPU)* і нейронних механізмів *Apple*), помітного скорочення екологічних витрат (енергоресурсів, води), розвитку самонавчання (метанавчання) ШІ, розвитку компактних ШІ (приміром, для смартфонів, транспорту), як і високошвидкісних міжсистемних з'єднань, масштабованої хмарної інфраструктури та ін.

Вищевикладене свідчить на користь твердження, що наслідки впровадження ШІ не просто примножать ефективність процесів у найрізноманітніших сферах та галузях, але, як переконують експерти та дослідники, сприятимуть створенню нових робочих місць та навіть нових галузей, як, наприклад, планування сталого розвитку на основі ШІ. Стає зрозумілим уже сьогодні: низка сучасних професій під тиском ШІ зникне. Серед перших, хто стане непотрібним, на думку фахівців з *OpenAI*, будуть бухгалтери, податкові фахівці, помічники юристів, фінансові аналітики, журналісти, веб-дизайнери, математики, судові репортери, перекладачі та спеціалісти зі зв'язків з громадськістю.

Тож, прогрес вимагатиме перекваліфікації співробітників, оскільки робота з ШІ вимагатиме нових знань, навичок, умінь, висуватиме нові вимоги до спроможностей та організації кожної особистості впродовж всього життя, чи того його періоду, впродовж якого особистість буде прагнути залишатися поза *класом "непотрібних людей"*.

На жаль, *клас "непотрібних людей"* — явище, яке розширюватиметься внаслідок розвитку ШІ. Цьому сприятиме кілька чинників.

По-перше, неготовність самого працівника змінюватися, опановувати впродовж життя нове знання, набувати нові уміння, одне з яких пов'язане зі знанням англійської мови. Адже, як відзначають експерти [11], на кінець 2024 р. ШІ — переважно англомовний, а всі "гучно презентовані інструменти ШІ" (включно зі *GPT-4o*), за допомогою яких ми можемо спілкуватися

чи робити запити, “жахливо працюють не англійською”. Коли, наприклад, ви цікавитеся у ШІ арабською рецептурою страви, то він повідомляє запитуючому ознаки хвороби, а запит про японський фестиваль родючості (відомий і як фестиваль фалоса) може призвести до цензури і бану, оскільки ШІ ігнорує місцевий культурний або політичний контекст, соціальні традиції, і запит, відповідно, сприймає запит як такий, що не узгоджується з політикою використання *OpenAI.* Тож, незнання саме англійської, щонайменше, половиною людства відділяє цю половину від прогресу, заможнішого життя та занадто звужує життєві перспективи. Іншими словами, особистості важливо подолати мовний бар’єр: мовний бар’єр є бар’єром до англоцентричних технологій, бар’єром для зростання власної ефективності та, врешті-решт, благополучнішого життя, бар’єром для перебування поза межами *“непотрібних людей”*.

Інший акцент аналітиків ще більш промовистий: нинішні тенденції у розвитку ШІ “нічим не відрізняються від етноциду, спричиненого гонитвою за ШІ”, оскільки здійснюване навчання ШІ на англомовних джерелах сприяє сприйняттю ШІ моралі, норм, стандартів, світоглядних рамок англомовного західного світу (станом на 2024 р. англійська була найпопулярнішою мовою вебконтенту, на неї припадало майже 52,1% сайтів; друге місце посіла іспанська — 5,5% веб контенту, третє — німецька з 4,8%. На такі мови, як індійська, перська, китайська та індонезійська, якими розмовляло близько 2,7 мільярда людей, припадало приблизно по 1,5% веб контенту), а висновок зводиться до того, що “можливо, ШІ не вб’є людство, але він точно вб’є те, що робить нас людьми, — нашу культуру, якщо ми не приділимо увагу цій проблемі” [11]. Таким чином, брак великого масиву високоякісних текстів (від художніх творів і наукових публікацій до новин і технічної документації) для навчання генеративного ШІ зменшує, а то й унеможливлює розвиток ШІ певними мовами. І ця проблема на даний час, вочевидь, має слабкі перспективи для розв’язання.

Ще одним негативним наслідком своєрідної “мовної упередженості” ШІ є не лише те, що, спілкуючись не англійською, ШІ вимагає від користувача, як відзначають фахівці галузі, значно більше токенів (мінімальних одиниць даних) для запиту, а й те, що користувач, у підсумку, не отримує якісної новітньої інформації. Неефективна токенізація обертається подорожчанням кінцевого результату, чого багато держав не можуть собі дозволити. Тож, нині дається взнаки як відокремлення людини від інформації та передових технологій, так і глибокий технологічний розрив між державами та цілими регіонами планети, що продовжує неухильно поглиблюватися, а прискіпливий аналіз низки процесів піднімає окрему проблему — розвитку “цифрового колоніалізму” (див. про це детальніше в: [12]). Зокрема, Н. М’яле [13], використавши концепт “діджитал-імперій”, прогнозував, що ШІ стане інструментом концентрації влади на планеті у найпотужніших гравців, якими він розглядав США та КНР. Інші ж регіони (зокрема, Європа) стануть “кібервасалами” чи “кіберколоніями”. А. Бредфорд, рефлектуючи

щодо питання "цифрових імперій", звертала увагу на прагнення цих, останніх, фактично нав'язувати власні правила гри щодо ШІ іншим гравцям та, відповідно, домінувати над ними [14]. Крім того, коли мова заходить про використання "англомовно-упереджених" моделей ШІ у незахідному світі, то виникають значні ризики для безпеки, адже "шкідливі відповіді", створені ШІ не англійською, зростають до 35%, а точність виконання інструкцій знижується до 80% [11]. ШІ може продукувати прямолінійно-образливі чи значною мірою токсичні висловлювання. Або брехати, стверджуючи, наприклад, що російська пропагандистська фраза в автоперекладі українською ("нема сечі терпіти ці пекельні борошна") є ідіоматичним виразом, "глибоко вкоріненим в українській мові та культурі з елементами, які можна простежити до старослов'янських висловлювань" [11].

У недалекій перспективі ШІ зумовить ситуацію, пов'язану із переміщенням і створенням робочих місць. І цей баланс буде критичним. А вже сьогодні ШІ надає непропорційні переваги певній частині людства, яка спроможна до адаптації в умовах новітніх викликів і можливостей, виявляє високу здатність до мобілізації ресурсів та, врешті-решт, економічної першості та геополітичної гегемонії.

За такої ситуації актуальності не втрачає книга "Вакансія: людина. Як не залишитися без роботи в добу штучного інтелекту", написана Т. Девенпортом та Д. Корбі ще у 2018 р. У ній автори запропонували своєрідну стратегію виживання людини — аугментацію, та кроки "вгору—вбік—всередину—вузькою стежкою—вперед". Вони аргументували, що людина, яка: *(а)* залишить за собою виконання найскладніших інтелектуальних задач і буде здатна оперувати ширшими, ніж ШІ, категоріями та, відповідно, приймати рішення в умовах, коли бракує даних, *(б)* виявить здатність спиратися на "людський фактор" та психологію, а також працювати в "партнерстві" зі ШІ та домінувати над ним, коли варто виходити за межі суто раціонального підходу, *(в)* зможе контролювати ефективність ШІ, своєчасно втручаючись та коригуючи його роботу, *(г)* матиме глибокі знання і досвід у вузькій специфічній сфері, яку буде просто економічно недоцільно автоматизувати, *(д)* виявить здатність до розробки нових розумних машин, до впровадження технологічних інновацій тощо, залишиться затребуваною, оскільки цінність людського інтелекту перевершуватиме "цінності ШІ", який має працювати у "чорнових" процесах. Однак, якість людського інтелекту вимагатиме нових освітніх стратегій. Як вимагатиме актуальних стратегій, підходів, політик і кожна сфера функціонування людей та соціумів.

Коли йдеться про безпеку, аналітики, чи не найперше, акцентують, що національна безпека як система інституційних державних заходів задля забезпечення фізичного, соціального та економічного добробуту населення і збереження національного суверенітету у контексті тиску зовнішніх та внутрішніх загроз є, за влучним виразом Річарда Даррока [15], "змістом і підсумком" *raison d`etre* держави. Утім, специфічним наголосом сьогодення є те, що сучасна держава функціонує у гібридному безпековому середовищі з

його численними загрозами, особливістю яких є їх складність: не лише, власне, гібридність, але й швидка змінюваність (наприклад, поява наприкінці січня 2025 р. "чорного лебедя" — нової моделі ШІ від китайської компанії *DeepSeek*, що виявилася не просто рівною провідним американським моделям, але дешевшою та не вимагала значних обчислювальних потужностей, що дало можливість говорити про "китайський виклик" принципам сучасного технологічного лідерства; на початку березня поточного року світ дізнався про нового чат-бота зі штучним інтелектом під назвою *Manus*, творцем якого стала китайська компанія *Butterfly Effect*, яка заявила що її технологія перевершує *OpenAI*, творця *ChatGPT*, невизначеність тенденцій навіть у найближчому майбутньому. Кім того, взявши, для прикладу, сучасні підходи до осмислення не просто "найдавнішого заняття людства" — *війни*, а *війни майбутнього*, з'ясуємо, що її складність відтворюється уже на етапі рефлексій, оскільки дослідники розмірковують над широким спектром питань і, зокрема, про "екологію насильства", "приватизацію війни" чи "крихкість держави" ("занадто крихка, щоб утримати світ"), про "детериторіалізацію і насильницькі мережі". До того ж, рефлексії відбуваються у межах новітніх концепцій "нерегулярних та нетрадиційних бойових дій", "проксі-", "дистанційних" та "заступних" воєн, "гібридних" і "постмодерних", або "диких", зрештою — "квантових", "проти космічних" (про що промовисто говорить "Довідник Рутледжа про майбутнє війни", що побачив світ у 2024 р. [16]). Крім того, своєрідному ускладненню війни як явища і сьогодні, і в майбутньому сприятиме її *структурна складність* («війна, не-війна та місце між ними»), як і *складність її "компонентів"*: місця/ролі "статі у майбутніх війнах", "інтелекту і обізнаності", "військового штучного інтелекту" тощо.

Рефлексії над *складністю*, яку примножує ШІ, нині зосереджуються на проблемі появи загального ШІ та супер-ШІ, оскільки вони сприятимуть появі нових численних складнощів у функціонуванні та осмисленні гібридної реальності. Якщо перший, загальний ШІ, мислиться як "рівний людині", тобто як модель, яка буде спроможною робити все, на що здатна людина, то суть суперінтелекту витлумачується як здатність моделі перевершити людські здібності і досягти "рівня бога". А небезпека полягає в тому, що супер-ШІ здатний змінювати безпекове середовище. Застереження стосується того, що супер-ШІ зможе діяти "дуже довго й непомітно, вносячи малі зміни у світобудову" — у політичну структуру, законодавство, виробництво спеціальних речей, які в перспективі будуть потрібні самому супер-ШІ) [17], і яких людина просто не помічатиме доти, доки ШІ трансформує упередження щодо людини безпосередньо в біотероризм.

Усвідомлюючи, що прогрес не зупинити, експерти — у постійному пошуку засобів, які убезпечать від "повстання машин". Своєрідним "рецептом безпеки" стає пропозиція: залишатися "якомога менше залежним від усього, що пов'язано з інтернетом, комп'ютерами", і пам'ятати, що, приміром, системи *SmartHome* (які спроможні "наглухо зачинити вхідні двері, контролювати газопостачання чи роботу обігрівача") можуть стати небез-

печними [17]. Тобто автономія людини — шанс на її виживання у гіпотетичному протистоянні з супер-ШІ. У зв'язку з цим виникає нескінченна низка запитань… Чи вдасться у цьому протистоянні людині зберегти саму себе, чи ж їй доведеться погодитися на роль "молодшого партнера ШІ"? Чи відбудеться трансформація людини і її критичне перетворення, результатом якого буде симбіоз (гібрид) людини з ШІ? Якою мірою цінитиметься те, що постало не в результаті "AI-made", але "mind-made"? Яким чином трансформуватимуться у такому випадку політичні системи і режими в державах — у бік поглиблення демократичних процесів за допомогою ШІ, чи навпаки — у напрямку розростання і зміцнення на планеті авторитаризмів?

Заглиблення у ситуацію знову актуалізує питання, пов'язане з пріоритетами політичних еліт в умовах того чи іншого (демократичного чи авторитарного) політичного режиму, тих чи інших культурних і релігійних традицій — протестантизму і конфуціанства, індивідуалізму і колективізму (на що звертали увагу І. Хайн та Л. Флоріді [18]), або — "в режимі хаосу" і скорочення *простору свободи*. А наслідком є постання "ШІ-тократії", як показали, аналізуючи досвід Китаю, М. Берая, Е. Као, Д. Янг та Н. Юхтман [19]. Тож, на порядок денний виходить питання аналізу намірів тих, хто приймає політичні рішення: вони націлені на сприяння єдності суспільства, розвитку його освіченості, інтеграції (в умовах специфічного тиску прогресу і нескінченної появи технологічних інновацій), чи ж навпаки дії еліти виказуватимуть, якщо не на відверту байдужість до соціально значимих проблем, то на її аморальну зацікавленість у створенні та неухильній підтримці нездоланних інтелектуальних бар'єрів та, відповідно, у закріпленні в суспільствах ліній розламів, сформованих, зокрема, в результаті відсутності якісної освіти для більшості в суспільствах та нерівного доступу до ШІ, як і можливостей його використання. Наслідком буде не лише мінімізація *простору свободи*, але й розширення всередині держав кола (чи й мас) "нових рабів", "нових кріпаків" чи ще якихось "нових залежних", малоспроможних до критичного мислення.

Інший рецепт для убезпечення від деструктивного всевладдя ШІ — поширення практики постійної перевірки людиною на адекватність будь-якої інформації, презентованої на ШІ-смітниках — у численних медіа, соціальних мережах тощо, оскільки проблема можливостей і обмежень ШІ у створенні та поширенні дезінформації стала однією з пріоритетних для осмислення, про що свідчать численні публікації [20—23]. Так, у статті Е. Пауельс, що побачила світ зовсім недавно – у грудні 2024 р. [21], — зауважувалося те, що генеративний ШІ робить інформаційні війни як потужнішими, так і доступнішими, оскільки (у поєднанні зі збором даних) пропонує нові методи "індустріалізації наступального використання дезінформації"; а інтеграція генеративного ШІ з іншими потужними технологіями примножує і ускладнює потенціал інформаційної війни: ШІ використовується як зброя. Д. Колон [22], своєю чергою, звертав увагу на те, що прогрес у розвитку ШІ відриває нові способи підриву суспільств, зокрема, демократичних, які сповідують

принцип свободи інформації та тим самим ризикують створити сприятливі умови для намірів супротивників, пов'язаних із дестабілізацією. Важливому аспекту проблеми "ШІ-дезінформації", пов'язаному із інфодеміологією, з питанням використання ШІ для генерування та виявлення дезінформації присвячена монографія В. Моу та К. Градона [23], в якій автори, досліджуючи множину онлайн-взаємодій (поширення неправди в онлайн-спільнотах), висвітлили, як формуються посилання, як поширюється інформація та як, зрештою, вона впливає на думки та дії користувачів. Фактично, В. Моу та К. Градон дослідили "кухню" когнітивних воєн, що розгортаються за допомогою ШІ в середовищі онлайн-спільнот.

Серед інших пріоритетів аналізу особливостей розвитку ШІ — проблема кібербезпеки, сфери, в якій ШІ стає невід'ємною частиною і виявляє свою специфічну подвійність. З одного боку, ШІ у режимі реального часу здатний аналізувати величезні обсяги даних, виявляючи аномалії та запобігаючи порушенням (спричиненим, приміром, хакерськими атаками), що здатні призвести до ескалації загроз, та, відтак, спроможний швидко ізолювати пошкоджені елементи системи та виправляти їх. З іншого боку, ШІ є потужним інструментом у руках злочинців, які практикують всезростаючі (у кількісному і якісному вимірах) фішингові схеми, вдало імітуючи надійні джерела інформації, так чи інакше ошукуючи користувача. Таким чином, дається взнаки протистояння між ШІ, який захищає, і ШІ, використаним зловмисниками, що зумовлюватиме динамічну зміну безпекового середовища та вимагатиме постійного оновлення/вдосконалення систем безпеки.

Особливо варті уваги дослідження, присвячені сучасній та майбутнім війнам у контексті їх трансформації, з огляду на все більшу значущість у них, як стало очевидним і незаперечним у ході російсько-української війни, дистанційної компоненти. Ця, остання, з-поміж іншого, забезпечується саме використанням ШІ, оскільки технологія має характеристики технології подвійного призначення, про що переконливо писали Х. Уено [24; 25] та вищезгадана Е. Пауельс [21].

Аналітики звертають увагу, щонайменше, на три моменти використання ШІ для потреб війни:

перший, пов'язаний із рефлексією над проблемою, півтора десятки років тому своїм способом окресленою А. Крішнаном — про "автономність зброї та штучний інтелект" [26], прискіпливо розглянутою в 2016 р. у праці М. Горовіца [27], у 2019 р. — П. Асаро [28], сьогодні ж осмислюваної під дещо іншим кутом зору — у площині про ступінь заміни людини ШІ в ході виконання тактичних, оперативних і стратегічних завдань. Професійні дискусії точаться довкола питання "корисності ШІ", а окремим акцентом стає думка про те, що зростаюча роль ШІ у системах озброєнь змінює правила гри [29]. Як і наголошується й інший факт: наслідком війни з підтримкою ШІ стане її тривалість та заплутаність [30];

другий момент стосується використання ШІ для аналізу даних та статистичних прогнозів. Експерти [31] схиляються до того, що ШІ є швидким

і ефективним, оскільки здатний зменшити громіздкі операції, здійснюючи передбачення в умовах небойових дій та процесів. Разом з тим виникає проблема, пов'язана зі здатністю ШІ обробляти події реального часу, які перебувають у розвитку: ШІ здатний видавати неточні або й недоречні дані, як це було у випадку замаху на кандидата у президенти США від Республіканської партії Д. Трампа, коли ШІ корпорації *Meta* (що об'єднує *Facebook*, *Instagram* і *WhatsApp*) помилково заперечував факт замаху;

зрештою, третій момент засвідчує концентрацію уваги дослідників на проблемі прийняття рішень у площині "людина *versus* ШІ" [31]. Обґрунтовується думка, що передбачення/прогноз з використанням ШІ є лише одним з аспектів ухвалення рішення. Інші дві важливі складові процесу ухвалення — дані та судження. Тільки людині (зацікавленій стороні) варто визначати, які дані є корисними, значущими та за яких умов/контексту. Тож, лише за умови наявності якісних даних, осмислених суджень, які охоплюють наміри командування, адміністрування та правила залучення, як і моральне лідерство, "вузький" ШІ здатний покращити процес прийняття рішень.

Досліджуючи військові інновації, аналітики наголошують, що "технологія не є простою заміною військової сили", а технологічні можливості залежать від додаткових інституцій, навичок і доктрин [31]. У ході ж розвідувальних і оперативних завдань команди людей і машин можуть в оптимальний спосіб розподіляти "когнітивне навантаження у процесі прийняття рішень".

Разом з тим, аналізуючи практики "нового інтервенціонізму" (у рамках дистанційних воєн) експерти акцентують важливість осмислення різноманіття не лише наслідків бойових дій (приміром, безпілотників) в етичному, правовому, політичному контекстах, як і в соціальному та економічному, але звертають увагу на низку технологічних розробок, які керуються ШІ, виконуючи ті чи інші критичні функції. Зокрема, зазначається, що подібна зброя обробляє дані від бортових датчиків і алгоритмів для вибору (тобто для пошуку, виявлення, ідентифікації, відстеження або й знищення) і атаки (тобто задля застосування сили для нейтралізації, пошкодження чи знищення) цілей без втручання людини, що свідчить лише про одне: контроль людини усувається [30]. І така асиметрія, зрозуміло, породжує нові виклики і ризики. Найперше — зміниться не просто характер протистоянь, а трансформується баланс між державами світу, оскільки демократії, тримаючись за "закони" і "правила" ведення війни, однозначно програватимуть автократіям, не переобтяженим витрачанням часу на рефлексії про законність, етичність, гуманність ШІ [32; 33]. Утім, цікавий акцент: не лише авторитарні режими мають переваги і виступають як цифрові імперії, але й, як зазначала А. Бредфорд [14], своєрідними цифровими імперіями є й технологічні бізнес-корпорації, які здійснюють потужний вплив на цифрову економіку.

Проблемі спроможності демократичних і авторитарних режимів досягти переваг над супротивником за допомогою ШІ присвятили свої дослідження Б. Бюкенен та Е. Імбрі [32], Ф. Філгейрас [34], П. Шаре [35]. У центрі

уваги дослідників були таланти, дані, компутаційні потужності, інституції, особливості урядування як в демократіях, так і в авторитарних державах. У підсумку висновок як вищезгаданих, так і інших авторів, зводився до того, що авторитарна ієрархія сприяє кращим результатам у ході реалізації політики щодо розвитку ШІ.

Інший наголос досліджень [36; 37] — переформатування світу, як в час Холодної війни: США і КНР як дві "наддержави" провадитимуть гру з нульовою сумою за власну домінантну позицію в розробці технологій зі ШІ, а інший світ просто примкне до котрогось із лідерів.

Обстоюючи тезу про те, що "ШІ є екзистенційним пріоритетом для автократії, очолюваної Комуністичною партією Китаю", та стверджуючи, що Китай сьогодні виступає з не аби-якою "національною рішучістю" та як "повноцінний конкурент Сполучених Штатів у комерційних і національних безпекових застосуваннях ШІ", Г. Еллісон та Е. Шмідт [36] зауважили, що прагнення Китаю освоїти ШІ виходить далеко за рамки визнання того, що ШІ-технології обіцяють стати найбільшим рушієм економічного прогресу в наступній чверті століття та інструментом "для вдосконалення диктатури" та плану "зробити Китай знову великим" (що, зауважу принагідно, суголосне намірам Д. Трампа щодо США). При цьому, що прикметно, претендуючи на гегемонію у світі ШІ-технологій, Китай не має тих конституційних та ціннісних обмежень, які є стримуючим чинником для США; у китайців, на відміну від американців, немає страху перед "державою спостереження" та її доступом до особистих даних, перед камерами у "розумних містах", що спостерігають за громадським та приватним життям (згідно з програмою "Гострі очі") та задовольняють безпекові потреби китайців (на противагу американцям, які "погоджуються на щомісячні масові розстріли"). Нагадали дослідники і застереження колишнього генерального директора Google Е. Шмідта про те, що якби Совєтський Союз зміг використати "складне спостереження, збір і аналітику даних, якою сьогодні користуються керівники Amazon, він цілком міг би виграти холодну війну".

Вищезгадані, як й інші численні факти, змушують одних експертів говорити про крихкість американського лідерства у сфері ШІ. Інших — про залежність КНР від демократичних держав-виробників чипів на фоні амбітного плану китайців — стати світовим лідером галузі до 2030 р., "глобальною супердержавою ШІ" (як писав Дж. Цзенг у дослідженні 2022 р., присвяченому ШІ з китайською специфікою в умовах "федералізму у китайському стилі", з його фіскальною децентралізацією, яка, як стверджував автор, була "ключем до економічних чудес Китаю за останні десятиліття" [37]). Крім того, варта уваги й думка, суть якої зводиться до того, що протистояння лише двох країн — США і КНР — перебільшене, але поширення наративів про цю конкуренцію є вигідним іншим учасникам ШІ-перегонів, тим, які не зацікавлені, як у захисті даних, так і в законодавчому регулюванні ШІ [38].

Таким чином, вищевикладене дає можливість твердити, що розвиток штучного інтелекту несе в собі як нові можливості для людства, так і новітні

виклики, загрози, ризики. Зокрема — у багаторівневій сфері безпеки, оборони, розвідки. І хто краще скористається перевагами ШІ — демократії чи новітні авторитаризми — покаже лише час.

3.2. Потенціал держав у розвитку та застосуванні ШІ: переваги та обмеження демократій та автократій

З 2018 р. Китай став своєрідним епіцентром уваги до ШІ, оскільки в Шанхаї за підтримки Організації промислового розвитку ООН почала проводитися щорічна Всесвітня конференція зі штучного інтелекту [39] заради того, щоб "допомогти зробити ШІ каталізатором інклюзивного та сталого промислового розвитку в усьому світі". У тому ж — 2018-у — році, як відомо, Кай-Фу Лі видрукував нині широковідому книгу під назвою "AI. Наддержави штучного інтелекту: Китай, Кремнієва долина, новий світовий порядок" [40], сама назва якої своїм способом визначила, щонайменше, три тенденції сучасності: по-перше, нову хвилю інтересу до штучного інтелекту; по-друге, окреслила основних гравців/конкурентів на полі ШІ — Китай та США, які, акцентую, на той час були уособленням двох протилежностей — демократії і авторитаризму; зрештою, книга, і це — по-третє, по-своєму сповістила про настання нового світового порядку.

Цей новий світовий порядок характеризується не лише крахом міжнародної безпекової чи правової систем та розгортанням у Європі найбільшої з часу після Другої світової війни агресії — росії проти Української держави, але й деградацією демократії в загальнопланетарному масштабі. Про це красномовно свідчив оприлюднений 27 лютого 2025 р. *Index Democracy* [41], згідно з яким, демократія у світі перебуває у найгіршому стані за останні 20 років. Тобто — з 2006 р., коли згаданий індекс був укладений вперше щодо 167 країн та територій. З того моменту країни класифікуються за п'ятьма критеріями і поділяються, відповідно, на чотири категорії — повна демократія, демократія з недоліками, гібридні режими та авторитарні режими. З врахуванням цього, з точки зору *Economist*, загальносвітовий рівень демократії був найвищим у 2015 р. і становив 5,55 балів (за шкалою від 0 до 10, де 0 — найнижчий показник). Нині показник демократії спустився до рекордно низького рівня і становить 5,17. Тож, якщо десять років тому 12,5% населення планети проживали в умовах повної демократії, то нині — лише 6,6%, а приблизно двоє з п'яти людей живуть в умовах авторитаризму [41].

Факт занепаду демократії і посилення авторитаризму непокоїть не тільки через зменшення простору свободи, але й, зрозуміло, через те, що новітні технології, і в тому числі ШІ, стають впливовим інструментом, спрямованим проти найрізноманітніших свобод людини і спільнот.

Інша тенденція нашого часу — потужні збройні конфлікти на планеті, яких, за даними *SIPRI*, у 2023 р. хоч і поменшало, порівняно з 2022 р. — 52 проти 55, утім, оціночне число загиблих у їх наслідок у світі зросла зі 153 100 осіб у 2022 р. до 170 700 осіб у 2023 р., сягнувши найвищого рівня з 2019 р. [42].

При цьому у 2023 р. чотири конфлікти, у т.ч. — громадянські війни в М'янмі та Судані; війни Ізраїлю з ХАМАС і росії з Україною, були віднесені фахівцями *SIPRI* до категорії крупних збройних конфліктів (тобто конфліктів з 10 000 і більше загиблих унаслідок конфлікту на рік), що на один більше, ніж у 2022 р. Кількість збройних конфліктів високої інтенсивності (з числом загиблих від 1 000 до 9 999 осіб) теж зросла — з 17 у 2022 р. до 20 у 2023 р.

Осмислюючи особливості підходів до розвитку і застосування ШІ у світі, де демократія згортається, панує несприятливий геополітичний клімат, а дипломатія слабшає (остання домовленість про припинення вогню була підписана майже десятиріччя тому — у 2016 р. між колумбійським урядом та повстанцями лівого руху ФАРК), але масштабується кіберзлочинність, загострюються питання щодо відповідальної торгівлі зброєю та товарами подвійного призначення і, відповідно, діяли/діють ембарго ООН (у 2023 р. — 14) та ЄС (у 2023 р. — 22, у тому числі 8 ембарго, що не мли відповідника в ООН: щодо Білорусі, Венесуели, Єгипту, Зімбабве, М'янми, Китаю, росії та Сирії [42]) на постачання зброї, а крім того, діяли режими експортного контролю (Австралійської групи — щодо хімічної та біологічної зброї; Режиму контролю над ракетними технологіями, Групи ядерних постачальників і Вассенаарської домовленості щодо контролю над експортом звичайних озброєнь, товарів і технологій подвійного використання), візьмемо до уваги те, що за таких умов відсутнє будь-яке загальноприйнятне визначення штучного інтелекту, як відрізняються глосарії термінів ШІ[1*]. Крім того, в очі впадають відмінності у підходах до ШІ держав (про що по-своєму свідчить те, що росія є учасницею усіх режимів експортного контролю, окрім Австралійської групи) та бізнесу, державних і недержавних акторів. Як вартий уваги і той факт, що стратегії демократій щодо використання ШІ відрізняються від стратегій авторитаризмів на тлі постійного збільшення військових витрат (у 2023 р. — 2443 млрд дол. [43]) і чіткої тенденції мілітаризації світу.

Зосереджуючись на питанні визначення лідерів у сфері технологій штучного інтелекту, зауважу, що останніх виокремлюють і оцінюють за різними критеріями. Найперше — за кількістю винаходів. І тут, що показово,

[1] Як повідомляв у серпні 2024 р. американський Інститут Брукінгса, з 2019 р., власне, Інститут Брукінгса і Центр міжнародної безпеки та стратегії Університету Цінхуа (КНР) збирають групи експертів із технологій національної безпеки у США та Китаї для неофіційного діалогу Track-II щодо штучного інтелекту, оскільки виникла потреба у створенні паралельних глосаріїв термінів ШІ (один розроблений американськими експертами, а інший — китайськими) задля забезпечення точного розуміння одними інших під час обговорення ШІ та проблем національної, як і міжнародної безпеки, стабільності та військових справ. Передбачається, що в ході розвитку технології, державних доктрин та практик надані визначення вимагатимуть подальшого уточнення та змін, згідно з офіційною політикою [48]. До лютого 2024 р. відбулося 9 діалогових зустрічей. Глосарій-2024 охопив п'ять напрямів: зброя (системи); інтелектуальні/автономні платформи (системи); інтелектуальні/автономні технології; дію та контроль; людино-машинні відносини.

Китай став лідером у винаходах у сфері генеративного штучного інтелекту, зареєструвавши у період 2014—2023 рр. понад 38 тис патентів *GenAI*, тоді як США подали 6,8 тис заявок, а третє–п'яте місця у рейтингу посіли, відповідно Південна Корея, Японія та Індія [44].

Компанії, що працюють із ШІ-технологіями оцінюють і за показником вартості. Тож, на середину 2024 р. найдорожчою компанією в світі з вартістю 3,335 трильйона доларів стала американська *Nvidia*. *Nvidia* випередила *Microsoft* (вартістю 3,317 трлн дол.) і *Apple* (3,286 трлн дол.) [45]. Крім того, до уваги береться і критерій «впливовості». Так, восени 2024 р. до топ-десятки найвпливовіших компаній аналітики відносили: *DeepMind* від *Google*, *OpenAI*, *NVIDIA*, *Microsoft*, *Amazon*, *Meta (Facebook)*, *IBM*, *Grok/xAI*, *Tesla*, *Apple* [46].

Утім, наприкінці січня 2025 р. за критерієм «найкращі» компанії ШІ до топ-десятки увійшли: китайські компанії *Alibaba* та *Baidu*, які у рейтингу посіли, відповідно, 10-те та 9-те місця; місця з 8-го до 3-го посіли американські *IBM*, *Meta*, *NVIDIA*, *Alphabet*, *Anthropic*, *Microsoft*; 2-ге місце дісталося китайській *DeepSeek, а перше* – американській *OpenAI* [47]. Таким чином, саме американсько-китайська "ШІ-конкуренція" в останній час виразно набирає обертів, що викликає стурбованість через те, що ці дві держави не просто стратегічні супротивники, як неодноразово наголошували американці, але й мають найбільший військовий потенціал.

Крім вищевказаного, специфічні ознаки часу віддзеркалюють ще кілька інших моментів. Перший. У 2013 р. почалася кампанія протидії необмеженим роботам на полі бою, і в 2019 р. її вже підтримували 57 країн та 113 неурядових організацій [49]. Другий. Починаючи з 2015 р. до обговорення питання використання летальної автономної зброї в рамках Конвенції про певні види звичайної зброї долучилася ООН. Утім, США, Ізраїль та росія як країни-піонери в галузі автономних систем зброї відкидали обов'язковість їх заборони. Третій. Восени 2020 р., австрійці (першими серед країн Євросоюзу), розмірковуючи над морально-етичними нормами використання на полі бою роботів-убивць і безпілотників та висловлюючись на користь того, щоб люди, а не алгоритми "нулів і одиниць", вирішували питання життя і смерті, закликали [50] до створення міжнародної етичної системи, етичних правил, таких стандартів щодо роботів та безпілотників на полях битв майбутнього, які б були аналогічними тим, які свого часу були встановлені для наземних мін і касетної зброї. Загалом, на той час — осінь 2020 р. — вже 30 держав та Європейський парламент висловлювалися на користь повної заборони використання роботів-убивць [50].

Якщо спробуємо проаналізувати політику США в сфері ШІ, то варто зануритися у 2016 р., коли Національна науково-технічна рада (NSTC) випустила звіт "Підготовка до майбутнього штучного інтелекту" разом із "Національним стратегічним планом досліджень і розвитку штучного інтелекту" (план *R&D*). У звіті було здійснено огляд стану розробок та використання ШІ, як і була приділена увага питанням, які ШІ створював для суспільства та

державної політики, та у зв'язку з цим були дані рекомендації уряду. Другий документ містив опис семи стратегій щодо необхідних досліджень і розробок. У грудні 2016 р. їх було доповнено положеннями документу "Штучний інтелект, автоматизація та економіка", в якому описано потенційний вплив автоматизації на основі ШІ на американський ринок праці та економіку, а також рекомендації щодо політики, основою якої (у дусі протестантської етики) мала стати орієнтація та опора на ринкову капіталістичну економіку та інновації.

Серед основних подій, пов'язаних зі спробами унормування використання ШІ в наступний час, зверну увагу на виконавчий наказ Д. Трампа (11 лютого 2019 р.) "Збереження американського лідерства у сфері штучного інтелекту" [51], в якому наголошувалася думка про те, що "Сполучені Штати є світовим лідером у дослідженні та розробці (НДДКР) та розгортанні штучного інтелекту", та проголошувалося, що продовження американського лідерства у сфері ШІ є "надзвичайно важливим для підтримки економічної та національної безпеки … формування глобальної еволюції штучного інтелекту відповідно до цінностей, політики та пріоритетів… країни". У наказі, що складався із 10 розділів, зауважувалося, що для збереження лідерства в області ШІ необхідно:

узгоджених зусиль для просування прогресу в технологіях та інноваціях при одночасному захисті американських технологій, економічної та національної безпеки, громадянських свобод, конфіденційності і американських цінностей;

посилення міжнародного та промислового співробітництва з іноземними партнерами та союзниками.

Наказ закріплював тезу про те, що американська ініціатива ШІ буде керуватися п'ятьма принципами, згідно з якими США повинні:

(a) сприяти технологічним проривам у галузі ШІ "у федеральному уряді, промисловості та академічних колах, щоб сприяти науковим відкриттям, економічній конкурентоспроможності та національній безпеці";

(b) стимулювати розробку відповідних технічних стандартів і зменшувати перешкоди для безпечного тестування та розгортання технологій штучного інтелекту, щоб уможливити створення нових галузей, пов'язаних із ШІ, і впровадження ШІ в існуючих галузях;

(c) навчати нинішні та майбутні покоління американських працівників навичкам розробки та застосування технологій ШІ, щоб підготувати їх до сучасної економіки та робочих місць майбутнього;

(d) підтримувати громадську довіру до технологій штучного інтелекту та захищати громадянські свободи, приватне життя та американські цінності під час їх застосування, щоб повністю реалізувати потенціал технологій штучного інтелекту для американського народу;

(e) сприяти міжнародному середовищу, яке підтримує американські дослідження та інновації ШІ та відкриває ринки для американських галузей штучного інтелекту, одночасно захищаючи наші технологічні переваги в ШІ

та захищаючи наші критично важливі технології ШІ від придбання стратегічними конкурентами та ворогуючими націями.

Документ визначав шість стратегічних цілей у галузі ШІ: сприяння постійним інвестиціям у дослідження та розробку ШІ у співпраці з промисловістю, академічними колами, міжнародними партнерами та союзниками та іншими нефедеральними суб'єктами заради здійснення технологічного прориву у ШІ та пов'язаних технологіях та швидкого перетворення цих проривів у можливості, які сприятимуть економічній та національній безпеці США; розширення доступу до високоякісних і повністю відстежуваних федеральних даних, моделей і обчислювальних ресурсів для підвищення цінності таких ресурсів для досліджень і розробок ШІ, збереження безпеки, конфіденційності відповідно до чинних законів і політики; зменшення перешкод для використання технологій ШІ та для просування їх інноваційного застосування при одночасному захисті американських технологій, економічної та національної безпеки, громадянських свобод, приватного життя та цінностей; забезпечення технічних стандартів, які мають зводити до мінімуму вразливість від атак зловмисників і відображати федеральні пріоритети щодо інновацій, громадської довіри та довіри громадськості до систем, які використовують технології ШІ; навчання наступного покоління американських дослідників і користувачів ШІ (через учнівство, "програми навичок", освіту в галузі науки, технологій, інженерії та математики (STEM) з акцентом на інформатиці), щоб гарантувати, що американські працівники, включно з федеральними працівниками, зможуть повною мірою скористатися можливостями ШІ; розробка та впровадження плану дій (відповідно до Президентського меморандуму про національну безпеку від 11 лютого 2019 р. "Захист переваг Сполучених Штатів у сфері штучного інтелекту та відповідних критичних технологій"), заради захисту переваги США у ШІ та технологіях, які мають вирішальне значення для інтересів економіки та національної безпеки, від стратегічних конкурентів та іноземних противників.

Документ (3—8 розділи) визначав "ролі та обов'язки" суб'єктів процесу, певною мірою торкався питання федеральних інвестицій у дослідження та розробки ШІ, даних та обчислювальних ресурсів, містив настанови щодо регулювання застосування ШІ, використання "американської робочої сили", а також план дій щодо захисту переваг США в технологіях ШІ.

У 9-у розділі, що привертає увагу, було дано визначення поняттям ШІ та відкриті дані. Тож, ШІ враховував/означав "повний обсяг федеральних інвестицій у штучний інтелект, включаючи: дослідження та розробки основних методів і технологій штучного інтелекту; системи прототипів ШІ; застосування та адаптація методів ШІ; архітектурну та системну підтримку ШІ; кіберінфраструктуру, набори даних і стандарти для ШІ", а "відкриті дані" тлумачилися як "загальнодоступні дані, структуровані таким чином, щоб [вони] були повністю доступними для виявлення та використання кінцевими користувачами".

Іншою подією, вартою уваги, стала, зокрема, поява ініціативи "Штучний інтелект для американського народу" (2021), в якій піднімалося питання поєднання американських цінностей і ШІ. Аналізуючи цей, як і інші, документи, в яких мали місце рефлексії над питанням американських цінностей, експерти відзначали, що в них йшлося про "нечіткі та нестабільні цінності", які були "радше риторикою, ніж справжньою основою для доброго суспільства із ШІ" [18]. Такі зауваження звучали як "перші дзвіночки", як своєрідна пересторога не лише для суперників США, але й для партнерів чи союзників. Далі — більше. З одного боку, у низці документів американці зачіпали питання "надійності ШІ", та був присутнім наголос на "довірі до ШІ", зауважувалася потреба "рівного доступу" до нього. Але аналітики звертали увагу на інше — на "шовіністичну риторику" в деяких документах США. Її суттю був "туман" довкола "американських цінностей і геополітичної конкуренції", що підводило до висновку про те, що іноді "американські цінності… включають світове лідерство" та сприймаються як "націоналістичний заклик до посилення підтримки американського штучного інтелекту" [18].

Зусилля американців, спрямовані на розвиток ШІ у наступний час, віддзеркалив не лише американський сенатський форум — *AI Insight Forum*, який вперше запрацював 13 вересня 2023 р. і до кінця року відбувся 9 разів [52], але й указ американського президента Дж. Байдена (жовтень, 2023 р.) [53], який був націлений на досягнення низки цілей у сфері ШІ: створення нових стандартів та захисту ШІ; захист конфіденційності; сприяння рівності та громадянським правам; захист споживачів, пацієнтів, студентів; підтримка працівників; сприяння інноваціям та конкуренції; просування лідерства США в галузі ШІ-технологій; забезпечення відповідального та ефективного використання технологій американським урядом. Чільними ідеями указу стали ті ідеї, згідно з якими передбачалася розробка стандартів для захисту від використання ШІ для створення біоматеріалів, встановлення найефективніших практик автентифікації вмісту, крім того — розробка передових програм кібербезпеки. Передбачалося, що, наприклад, Національний інститут стандартів і технологій відповідатиме за розробку стандартів тестування моделей ШІ. На Міністерство енергетики та Міністерство внутрішньої безпеки покладався обов'язок забезпечення уникнення загроз ШІ для інфраструктури та впливу на хімічні, біологічні, радіологічні, ядерні ризики та ризики кібербезпеки. Промовистим моментом указу стала вимога до розробників ШІ, зокрема, таких, як *OpenAI* та *Meta*, ділитися даними з урядом.

Аналіз американських практик щодо ШІ дозволяє не тільки виявити тенденції у підходах до ШІ найпотужнішої держави світи, але й «зчитати» загрози, які можуть продукуватися США для світу у разі все більшої деформації демократії в країні.

Аналіз міжнародного контексту, в якому в останні роки розвивається ШІ, дозволяє твердити, що ключовими міжнародними зустрічами, зокрема, впродовж 2023 р. з проблематики ШІ стали такі, як:

світовий форум в Гаазі (15–16 лютого 2023 р.), яким було започатковано міжнародне зібрання з відповідального ШІ у військові сфері — *Responsible AI in the Military Domain, REAIM*, де обговорювалися питання щодо прозорості, тлумачення та упередженості у використанні прикладних програм ШІ, заснованих на машинному навчанні;

перше в історії офіційне засідання Радбезі ООН з питань ШІ в Нью-Йорку (18 липня 2023 р.), на якому наголошувався зв'язок ризиків і вигод ШІ-технологій;

саміт з безпеки ШІ у Великобританії (Блетчлі-парк, 1—2 листопада 2023 р.), учасники якого зосередилися на питаннях безпечної та відповідальної розробки передового ШІ в усьому світі.

Крім того, зверну увагу і на інші події, що мала місце наприкінці 2023 р.: ШІ був ключовим моментом двосторонньої зустрічі президентів Китаю і США (листопад, 2023 р.), а в Європі, у грудні 2023 р. [54], представники Європарламенту, Єврокомісії та держав ЄС після триденних переговорів досягли політичної угоди щодо регулювання штучного інтелекту та схилилися до думки, що європейці мають ухвалити закон про ШІ. Тож, невдовзі (березень, 2024 р.) депутати Європарламенту, сподіваючись на обмеження ризиків, пов'язаних із використанням ШІ, та бажаючи розвивати ШІ як більш людиноцентричну технологію, схвалили (вперше у світі) комплексний закон щодо ШІ. Е. Яннополло, головний аналітик *Forester*, наголосила, що закон є "набором зобов'язуючих вимог щодо пом'якшення ризиків штучного інтелекту", і такий підхід ЄС повинен стати «де-факто» глобальним стандартом для надійного ШІ [55]. Візьмемо на замітку, що закон був націлений на захист фундаментальних прав людини і захист верховенства права та демократії, забезпечення стійкості навколишнього середовища від ШІ з високими ризиками. Зокрема, заборонялися додатки зі ШІ, які могли використовуватися для біометричної категорізації громадян на основі конфіденційних характеристик і нецільового збирання зображень облич з Інтернету чи записів камер відеоспостереження для створення баз даних (з розпізнавання облич); додатки для розпізнавання емоцій на робочому місці та в школах, соціальної оцінки, прогнозної поліції, яка ґрунтується виключно на профілюванні особи чи оцінці її характеристик; додатки для маніпуляції людською поведінкою з використанням вразливих місць людини та ін. [56]. Крім того, що прикметно, це рішення європарламентарів мало на меті стимулювання інновацій в сфері ШІ та водночас — утвердження Європи як лідера галузі.

Якщо подивитися на Великобританію, то навесні 2023 р. країна оприлюднила "білу книгу" за назвою "Проінноваційний підхід до регулювання ШІ" [57], у передмові до якої член парламенту та державний секретар з питань науки, інновацій та технологій М. Донелан зауважила, що, починаючи з 2014 р., її країна інвестувала 2,5 млрд фунтів стерлінгів у ШІ, а мета Великобританії — "стати науково-технологічною супердержавою до 2030 року", світовим лідером у "секторі штучного інтелекту з нашими цінностями про-

зорості, підзвітності та інновацій", "айрозумнішим, найздоровішим, найбезпечнішим і найщасливішим місцем для життя та роботи". Держсекретарка відзначила той факт, що Великобританія займала у 2023 р. третє місце у світі за дослідженнями та розробками ШІ. У країні була розташована третина європейських компаній із ШІ та вдвічі більше, ніж у будь-якій іншій європейській країні. А обґрунтована у "білій книзі" стратегія щодо ШІ була дуже гнучкою і передбачала співпрацю між урядом, регуляторними органами та бізнесом. Іншим акцентом було те, що британці, на відміну від країн-членів ЄС, не збиралися запроваджувати нове законодавство щодо регулювання ШІ, оскільки вважали, що «поспішаючи приймати закони занадто рано, … ризикуємо покласти надмірний тягар на бізнес», до того ж в умовах швидкого розвитку технологій, як зазначалося, потрібно зрозуміти нові та новітні ризики, "взаємодіяти з експертами, щоб переконатися, що ми вживаємо необхідних заходів" для уникнення загроз та ризиків, взаємодіяти з громадськістю, щоб зрозуміти її очікування, та продемонструвати здатність і готовність реагувати на проблеми.

Аналіз стратегій британців та американців щодо ШІ в наступний час дозволив експертам (навесні 2024 р.) небезпідставно твердити, що "у США та Великобританії фірми, що займаються штучним інтелектом, здебільшого регулюють самі себе" [58]. А медіа назвали знаменною [58] укладену у квітні 2024 р. угоду між Великою Британією та США щодо безпеки ШІ. Документом передбачалася співпраця двох країн у сфері тестування ШІ — розробкою методів оцінки безпечності інструментів із ШІ та систем, які їх використовують. У кожній з країн було створено Інститути безпеки ШІ, метою яких є оцінка систем ШІ як з відкритим, так і закритим кодами. Більше того: у листопаді 2024 р. Міністерство торгівлі США та Державний департамент вирішили [59] запустити міжнародну Мережу інститутів безпеки ШІ на першій зустрічі в Сан-Франциско, за допомогою якої США сподіваються "вирішити деякі з найактуальніших проблем безпеки штучного інтелекту" та уникнути "неоднозначного глобального управління, яке може перешкоджати інноваціям". Першими членами Мережі стали Австралія, Велика Британія, Європейський Союз, Канада, Кенія, Республіка Корея, Сінгапур, США, Франція та Японія. Пріоритетні сфери співпраці для членів Мережі проголошувалися такі, як дослідження безпеки ШІ, розробка найкращих практик для тестування та оцінки моделей, сприяння інтерпретації тестів передових систем ШІ та просування глобального залучення та обміну інформацією, на що уряди країн-членів та низка благодійних фондів виділили понад 11 млн дол. США.

Іншою важливою подією 2024 р. стало вересневе зібрання представників близько 60-ти країн, і в тому числі США, Франції, Німеччини, Великої Британії, України, що мало місце в Сеулі — другий у своєму роді саміт "Відповідальний штучний інтелект у військовій сфері" (REAIM; перший саміт відбувся в 2023 р. в нідерландській Гаазі). У Сеулі був підписаний "план дій", який регулює відповідальне використання ШІ на полі бою. Утім, близь-

ко 30 країн не підтримали документ. Зокрема – Китай. Показовим було і те, що, як писала *Deutsche Welle* [60], росія, як країна-агресорка, не отримала запрошення на саміт.

Прикметно, що в умовах китайського "федеративного авторитаризму" не було створено національного інституту безпеки штучного інтелекту [61], натомість подібні структури були створені місцевими органам влади Пекіну та Шанхаю. Загалом, китайці ще у 2013 р. заявили про свої наміри розробити ШІ, але лише з 2017 р. розпочали ретельно прокладати свій шлях у сфері розвитку і використання ШІ. Про це незаперечно свідчили такі документи, як "Трирічний план дій" та "План розвитку ШІ нового покоління", що з'явилися у 2017 р. [18]. Квінтесенція тогочасного китайського мислення (як і американського, чи європейського) полягала в тому, щоб до 2030 р. стати світовим інноваційним центром у сфері ШІ.

"Чотирнадцятий п'ятирічний план національного економічного та соціального розвитку Китайської Народної Республіки та нарис довгострокових цілей на 2035 рік" (2021) також не поминули увагою питання розвитку ШІ, розглядаючи його в контексті хоч і "важливої технології", але яка витлумачувалася "однією з багатьох", і яка, в дусі конфуціанських настанов і традицій, має працювати на благо "гармонійного суспільства".

Усередині липня 2024 р. відбувся третій пленум 20-го ЦК КПК, який закликав до "запровадження систем нагляду для забезпечення безпеки штучного інтелекту", а у вересні 2024 р. Китайський національний технічний комітет 260 з кібербезпеки вже випустив першу версію китайської "Рамкової концепції управління безпекою ШІ" (див. про це детальніше: [62]).

Але повернімося до США початку цього, 2025-о, року. Заради збереження передових обчислювальних потужностей та, відповідно, лідерства у сфері ШІ США та їхніх найближчих союзників, американський уряд у останні дні правління Д. Байдена ухвалив рішення щодо додаткового обмеження експорту чипів штучного інтелекту (відомих як графічні процесори *GPU*, що використовуються не лише в іграх, але здатні обробляти частини даних, що робить їх цінними для навчання та запуску моделей ШІ), фактично розділивши світ та віднайшовши нові способи блокування доступу до новітніх технологій для близько 120 країн, серед яких Сінгапур, Ізраїль, Саудівська Аравія, Об'єднані Арабські Емірати, Швейцарія та ін., на які поширюватимуться встановлені експортні квоти [63]. А таким країнам, як Китай, росія, Іран, Північна Корея, на які поширюється ембарго на поставки зброї, технології мають стати взагалі недоступними, оскільки передові чипи здатні посилювати військові можливості кожної з них.

Нові правила, можуть почати діяти через 120 днів після публікації, якщо адміністрація Д. Трампа не вдасться до їх перегляду. Утім, вони не зачеплять таких (з 18-ти визначених) союзників США, як, Австралія, Бельгія, Великобританія, Канада, Данія, Ірландія, Іспанія, Італія, Нідерланди, Німеччина, Нова Зеландія, Норвегія, Південна Корея, Тайвань, Фінляндія, Франція, Швеція, Японія [64].

Іншою подією початку 2025 р., вартою уваги, виявився глобальний саміт у Парижі (лютий, 2025 р.), на якому Велика Британія та США не приєдналися до міжнародної угоди про ШІ [65], яка, з-поміж іншого, була підписана десятками країн, включаючи Францію, Китай, Індію, та націлювала підписантів на "відкритий", "інклюзивний" та "етичний" підхід до розвитку технології [66]. Крім того, на саміті вперше зверталася увага на новітній виклик, пов'язаний з тим, що використання енергії штучним інтелектом найближчим часом — до 2027 р. — може зрости до рівня споживання електроенергії невеликими країнами (такими, як, наприклад, Нідерланди), що, зрозуміло, поставить останніх у специфічне становище. Попри це, британці пояснювали свою відмову підписання угоди занепокоєнням щодо національної безпеки та "глобального управління", а віце-президент США Дж. Ді Венс, своєю чергою, заявив делегатам у Парижі, що надмірне регулювання ШІ може "вбити індустрію", а також зауважив, що ШІ — це "можливість, яку адміністрація Трампа не змарнує" що "політиці сприяння розвитку штучного інтелекту" слід надавати пріоритет над безпекою [66].

Що ж до Великої Британії, то на Паризькому AI Action Sammit британці підписали угоди щодо стійкого розвитку та кібербезпеки.

Аналізуючи ситуацію, що склалася, медії відзначали [67], що тоді, як ЄС ухвалив закон, покликаний забезпечити безпеку і підзвітність користувачів технології ШІ, президент США Д. Трамп прибирає обмеження в цій сфері, розв'язуючи руки ІТ-індустрії. Про це по-своєму свідчать дії Д. Трампа, віддзеркалені в низці документів і повідомлень, що оприлюднені на сайті Білого Дому після його вступу на посаду. Зокрема, у січні 2025 р. — "Усунення перешкод для американського лідерства у штучном у інтелекті"(23.01.2025) [68]; наприкінці лютого — "Запрошення до публічного обговорення Плану дій щодо штучного інтелекту" (25.02.2025) [69]; у березні — "Президент Трамп ставить американських робітників на перше місце і повертає американське виробництво" (04.03.2025) [70]; "Президент Трамп перетворює Америку на виробничу наддержаву" (12.03.2025) [71] тощо.

В умовах сьогодення варто не залишати поза увагою продовження і розвиток американсько-китайської співпраці, про що красномовно говорить "Проміжний звіт про міжнародний діалог між Китаєм і США щодо штучного інтелекту та міжнародної безпеки" [72]. Таким чином, на початок 2025 р. продовжує формуватися і увиразнюватися ландшафт багатосторонніх та двосторонніх центрів управління штучним інтелектом.

Впадає в очі й те, що з початку двадцятих років XXI століття низка Європейських країн розробила ті, чи інші документи щодо політики в сфері розвитку ШІ. Зокрема, Польща ще у 2020 р. презентувала своє бачення розвитку ШІ на короткострокову, середньострокову та довгострокову перспективу, відповідно — до 2023 р., 2027 р. та після 2027 р. Поляки виокремили шість сфер використання ШІ [73]:

ШІ та суспільство: діяльність у цій сфері має зробити Польщу "одним із найбільших бенефіціарів економіки, заснованої на даних", а поляків — "сус-

пільством, яке усвідомлює необхідність постійного вдосконалення цифрових компетенцій";

ШІ та інноваційні компанії: передбачає "підтримку польських підприємств із ШІ", створення механізмів фінансування їх розвитку, співпрацю між стартапами та владою;

ШІ та наука: націлена на підтримку польської наукової та дослідницької спільноти в розробці міждисциплінарних завдань або рішень у сфері ШІ, заходи, спрямовані на підготовку кадрів експертів із ШІ;

ШІ та освіта: передбачаються заходи, що здійснюються від початкової освіти до рівня університетів і пов'язані з розробкою програм курсів для людей, яким загрожує втрата роботи внаслідок розвитку нових технологій;

освітні гранти ШІ та міжнародна співпраця: передбачається діяльність, спрямована на підтримку польського бізнесу у сфері ШІ та розвитку технологій на міжнародній арені;

ШІ та державний сектор: підтримка державного сектору в реалізації контрактів на ШІ, кращу координацію діяльності та подальший розвиток програм, зокрема, таких як GovTech Polska.

Амбіції Італії віддзеркалює "Італійська стратегія щодо штучного інтелекту на 2024—2026 роки" [74]. Документ свідчить, що країна прагне отримати вигоди від ШІ заради покращення економічного та соціального ландшафту, орієнтуючись при цьому на розробку антропоцентричних, надійних і стійких рішень ШІ, які б відповідали європейським цінностям. Серед пріоритетів Італії – досягнення конкурентних переваг та уникнення надмірної залежності від іноземних технологій; сприяння поширенню ШІ в різних секторах; інвестиції в проекти з високим ступенем ризику, які досліджують інноваційні технології та програми ШІ; просування проектів, які поєднують ШІ з іншими науковими дисциплінами для вирішення складних суспільних проблем у найрізноманітніших галузях — від державного управління, функціонування підприємств, до навчання і підвищення добробуту італійців, спираючись на скрупульозне планування, співпрацю, дотримання етичних норм. Загалом, "Італійська стратегія…", можна твердити, свідчить про комплексний підхід країни до інтеграції ШІ в структуру національної економіки та соціуму. Все це дозволяє аналітикам дійти висновку про те, що Італія готова стати лідером "у світовому ландшафті штучного інтелекту, забезпечуючи стале зростання та добробут суспільства" в епоху ШІ [75].

Іншим прикладом, вартим уваги, є Німеччина, не абиякий інтерес до якої виявили американці і, зокрема, аналітики з телекомунікаційної компанії *Cisco*. Аналізуючи (наприкінці грудня 2024 р.) ситуацію у ФРН, експерти *Cisco* відзначали, що німецькі компанії "погано підготовлені до ШІ" [76], оскільки лише 6% серед них демонструють оптимальну готовність до використання ШІ-технологій, а 29% — добре підготовлені. Висновок зводився до того, що у "міжнародному порівнянні Федеративна Республіка відстає", оскільки займає 6-те місце в Європі за ступенем готовності, а лідером є Великобританія з 10 % підприємств з "оптимальною готовністю", яка випередила

Італію, Іспанію та Швейцарію, які мають по 9%. Якщо враховувати компанії, які "оптимально і добре підготовлені" до запровадження ШІ, то Німеччина посяде третє місце після Великобританії та Іспанії.

Аудит американців зауважив, що Німеччина знаходиться попереду в розробці стратегій ШІ: 95% компаній мають план боротьби з ШІ, або займалися його розробкою. Однак, тільки 35% володіли методами вимірювання наслідків рішень на основі ШІ, а ¾ компаній на кінець 2024 р. не мали правил використання ШІ. Тож за цим, останнім, показником Німеччина посідала лише 5-те місце. Слабким місцем німецьких компаній називалася фрагментація даних в компаніях та їх зберігання у різних сховищах. Хоча Німеччина посідала 2-е місце в європейському рейтингу інфраструктури, все ж зауважувалося її відставання оскільки компаніям не вистачало обладнання для ШІ. Слабкістю було і те, що тільки 40% компаній мали достатньо кваліфікований персонал, що відповідав необхідним вимогам.

Характерним було і те, що витрати на ШІ розподілялися фактично порівну між кібербезпекою, інфраструктурою та аналітикою даних. Крім того, зауважуючи, що майже п'ята частина німецьких компаній в найближчі п'ять років планує виділяти на ШІ 40% бюджету, фахівці Cisco акцентували, що попередні інвестиції в оптимізацію та автоматизацію процесів не виправдали сподівань [77].

З урахуванням стану ШІ в Європі, США та інших країнах, увагу привертають спільні зусилля компаній та урядів, спрямовані на розвиток ШІ. Так, на початку 2025 р. у США про себе заявила [78] нова компанія *Stargate Progect*, яка впродовж наступних 4-х років має намір інвестувати 500 млрд дол. США у створення нової інфраструктури ШІ для *OpenAI* у США, розбудова якої розпочалася з Техасу. Першими спонсорами інфраструктури стали *SoftBank, OpenAI, Oracle* і *MGX*. При чому японський *SoftBank* нестиме фінансову відповідальність, а *OpenAI* — операційну.

Новітній консорціум, до потужності якого придивляються аналітики з різних країн [78], буде здатним:

забезпечити американське лідерство у сфері штучного інтелекту;

створити сотні тисяч нових робочих місць;

принести «величезну економічну вигоду для всього світу», як впевнені американці.

Іншою метою "Зоряної брами", про підтримку якої заявив Д. Трамп, проголошено:

підтримку реіндустріалізації США;

забезпечення стратегічного американського потенціалу для посилення національної безпеки Америки та її союзників [78].

Щодо технологічних партнерів, то ключовими серед них названо *Arm, Microsoft, NVIDIA, Oracle і OpenAI*.

Показово, що, якщо в самих США про невіру у спроможність *OpenAI, SoftBank* та *Oracle* виконати свої обіцянки заявив І. Маск, то поза межами США американське лідерство у сфері ШІ по-своєму висловили готовність

оспорити низка країн. Так, у Німеччині, яка ще в часи, коли посаду канцлера обіймала А. Меркель, проголошувалося, що "ШІ зроблено в Німеччині" повинно було стати міжнародним брендом для "сучасних, безпечних, простих і хороших додатків штучного інтелекту на основі європейського канону цінностей" [79]. У 2018 р. Німеччина поставила три цілі: перетворення Німеччини та Європи "на провідне місце для розробки та застосування технологій ШІ" та забезпечення конкурентоспроможності Німеччини; "забезпечення відповідального та орієнтованого на загальне благо розвитку та використання ШІ", зрештою, проголошувалася необхідність того, шо ШІ "має бути вбудованим у суспільство етично, юридично, культурно та інституційно" як частина "широкого соціального діалогу та активного політичного дизайну" [79]. Задля досягнення цих цілей, федеральний уряд вважав за необхідне посилити дослідження та "прискорити передачу результатів досліджень в економіку"; створити "інфраструктуру даних як центральну основу для додатків ШІ"; збільшити кількість кваліфікованих робітників і експертів; активно формувати структурні зміни в компаніях і на ринку праці та в адміністраціях, створити "хороші рамкові умови для етичного застосування штучного інтелекту", розширювати європейське та міжнародне співробітництво з питань ШІ та сприяти веденню соціальному діалогу про можливості та вплив ШІ [79].

На передодні цьогорічного лютневого саміту в Парижі про амбіції Франції щодо першості в сфері розвитку ШІ заявляв Е. Макрон, оголосивши про інвестиції у розмірі 109 млрд євро в цю галузь заради того, щоб зміцнити позиції і Франції, і загалом Європи у глобальному технологічному змаганні [80].

Бажання першості в сфері ШІ країн Європи, США чи Китаю викликає певний сарказм і скепсис у японців, які на старті 2025 р. зауважили, що, коли світ говорить про ШІ, то у центрі уваги майже завжди потрапляють Сполучені Штати та Китай, а потім додали, що і перші, і другі — "самопроголошені технологічні титани". Саме з таких акцентів розпочинався оприлюднений у січні документ "Розквіт штучного інтелекту в Японії: повний путівник на 2025 рік" [81]. Оцінюючи ситуацію, японці зауважили, що поки США та Китай борються за переваги, то "на Сході з'явився тихий руйнівник, Японія", яка давно відома своєю "точною інженерією, культурою винахідливості, революціонізує штучний інтелект" і робить це "з прихованим блиском, який став її фірмовою ознакою". Тож, за переконанням японців, їх країна перетворюється "з гравця, якого не помічають, на стратегічну державу", адже Японія не просто "приєднується до гонки ШІ, але перевизначає її", намагаючись "перехитрити глобальних важковиків", і світові "варто звернути увагу на цю зростаючу наддержаву ШІ".

Як видатного гравця у світовому ландшафті ШІ позиціонує себе Південна Корея, яка ще наприкінці 2019 р. оприлюднила "Національну стратегію розвитку штучного інтелекту" та низку інших ініціатив. Вартий уваги і південнокорейський "Закон про штучний інтелект" (*SKAIA*) [82], ухвалений наприкінці грудня 2024 р. Національними зборами країни і який має набути

чинності з січня 2026 р. Він є своєрідним рамковим актом, що об'єднав 19 законопроєктів. Інша його особливість пов'язана з тим, що "Закон…" є другим у світі законодавчим актом щодо ШІ. Його цілі — забезпечення захисту прав і гідності людини та покращенні якості життя з одночасним зміцненням національної конкурентоспроможності країни шляхом встановлення правил для розробки надійного ШІ.

Зрештою, зверну вагу на стан запровадження ШІ в агресорці-росії. Ще у 2014 р. росіянами була запущена секретна комплексна цільова програма Міністерства оборони "Створення перспективної робототехніки до 2025 року", яка мала слугувати "керівною картою" для розвитку повітряної, наземної та морської робототехніки і в якій піднімалася проблема розвитку ШІ [83]. 26 липня 2022 р. російське Міністерство оборони прийняло "*Концепцію діяльності Збройних сил росії щодо розробки та використання систем озброєння з використанням технологій штучного інтелекту*", яку у березні 2023 р. росія оприлюднила в ООН. Експерти трактують "Концепцію…" як одну із основних "дорожніх карт" для впровадження в росії ШІ та відзначають той факт, що, незважаючи на труднощі, які росія "відчуває на українському полі бою та вдома, намагаючись підтримувати вітчизняні високотехнологічні дослідження та розробки штучного інтелекту", вона все ж виділяє "державні, академічні, промислові та фінансові ресурси для забезпечення розвитку свого ШІ", і ці "зусилля заслуговують на пильний і постійний контроль" [83].

Своєрідні підсумки щодо застосування ШІ підводить п'ята ітерація *Global AI Index*, опублікована у вересні 2024 р. [84]. Індекс обраховувався за 122 показниками із залученням даних із 24 різноманітних державних та приватних джерел у 83 державах. Показники розподілені на три "стовпи" (реалізація; інновація; інвестиції) та, відповідно, сім "під стовпів" (таланти, інфраструктура, оперативне середовище; інноваційні дослідження, розробки; урядові стратегії, активності — стартапів, інвестиції та бізнес-ініціативи на основі ШІ). Їх аналіз дозволив виокремити топ-десятку, до якої увійшли: США, КНР, Сінгапур, Велика Британія, Франція, Південна Корея, Німеччина, Канада, Ізраїль та Індія. Тобто, держави з різних регіонів планети та з різними — демократичними та авторитарними — політичними системами. Місця з 11 по 20 посіли такі держави, як Японія, Швейцарія, Нідерланди, Саудівська Аравія, Фінляндія, Гонконг, Австралія, Іспанія, Люксембург, ОАЕ.

Україна у рейтингу посіла 55-у позицію, а державам-сусідкам дісталися такі місця: 31-е — росії, 36-е — Польщі, 41-е — Угорщині, 50-е — Румунії, 66-е — Словаччині. Молдова та Білорусь до індексу не потрапили. Утім, зверну увагу, що до *Global AI Index* потрапили такі колишні совєтські республіки, як: Естонія (32-а позиція), Литва (46), Вірменія (65), Латвія (70) та Азербайджан (78).

Окрему увагу варто приділити звіту американської комісії зі сприяння розвитку штучного інтелекту (AAAI), що був підготовлений командою фахівців з 24 осіб, та опублікований зовсім недавно — у березні 2025 р. —

за назвою “Майбутнє досліджень штучного інтелекту” [85]. І ось така націленість в майбутнє і є головною особливістю документу. Якщо більш прискіпливо проаналізувати ключові акценти документу, що націлює дослідників, розробників та ін. спеціалістів із сфери ШІ на майбутнє, то виокремлю з-посеред них такі:

ШІ розглядається як система. А основні вимоги до цієї системи зводяться до того, що система ШІ повинна бути “реальною” чи “фактичною”, а відтак – надійною. Вона є “фактичною”, якщо “утримується від надання неправдивих тверджень”; “надійність” передбачає достовірність та зрозумілість наданої інформації і — особливий акцент! — спроможна враховувати “людські цінності”;

оскільки агентні та багатоагентні системи еволюціонували до інтеграції з генеративним ШІ та великими мовними моделями, це, зрештою, зумовить появу кооперативних структур ШІ. Важливою особливістю цих структур повинна бути значна адаптивність, здатність до масштабування, що забезпечуватиме співпрацю, переговори та етичні узгодження, а також створюватиме нові можливості для прийняття рішень та гнучкості. Інтеграція кооперативного ШІ з генеративними моделями вимагає збалансованої адаптивності, прозорості та обчислювальних можливостей у багатоагентному середовищі;

швидкий розвиток ШІ актуалізував проблему етичних та безпекових ризиків, пов’язаних з новими загрозами (наприклад, кіберзлочинністю, керованою ШІ). Аналіз новітніх загроз та ризиків вимагає уніфікованих підходів, оскільки спостерігається дедалі більша взаємопов’язаність короткострокових та довгострокових ризиків. “Проблеми етики та безпеки вимагають міждисциплінарної співпраці, безперервного нагляду і більш чіткої відповідальності у розробці ШІ”;

рефлексії над “втіленим ШІ” підводять до висновку, що “втілений ШІ” створює інтелектуальних агентів, які “сприймають, розуміють фізичний світ і здатні взаємодіяти з ним”. Розум виникає через з’єднання фізичного тіла з реальним середовищем;

у документі наголошується теза про те, що, з одного боку, ШІ «є чому навчитися в інших сферах когнітивної науки» як мультидисциплінарної галузі (про що уже свідчить сприйнята ШІ ідея когнітивної архітектури), а з іншого — і ШІ здатний зробити в останню “великий внесок”. Тож, розширення взаємодій може призвести до важливих успіхів в обох сферах;

успіхам ШІ сприятиме узгоджене проектування компонентів апаратно-програмної архітектури, яке й максимізує продуктивність, енергію, ефективність ШІ. Утім, розгортання систем ШІ на периферії залишається складним з кількох причин, серед яких “конкуруючі потреби в розподілі ресурсів і плануванні для інтегрованих систем та гетерогенному обладнанні, потреби в енергії та розсіювання тепла” тощо;

один із пріоритетів майбутнього — ШІ для соціального блага, що вимагає вимірювання його впливу на суспільство, особливо на вразливі вер-

стви населення, групи з обмеженими ресурсами, та, відповідно, його відповідальне використання. Цьому може посприяти "міцне партнерство між дослідниками штучного інтелекту, експертами в галузі, політиками та місцевими громадами" заради забезпечення довгострокової стійкості в умовах обмежених ресурсів середовища, що залишається ключовою проблемою;

наголошуючи, що ШІ "швидко трансформує індустрії та має величезні можливості для стимулювання прогресу сталого розвитку", фахівці звернули увагу, що розвиток теж породжує проблеми і, найперше, такі, як підвищення потреби в енергії та воді; екологічні ризики вимагатимуть активних зусиль;

відзначаючи, що ШІ революціонізує наукові відкриття шляхом прискорення всього дослідницького циклу, в документі обгрунтовано висновок, що ШІ прискорить темпи науки, оскільки відкриття відбуватимуться безпрецедентними способами, а процес пізнання докорінно трансформується: матиме місце мінімальне втручання людини у хід виконання визначених завдань, що актуалізує питання нової етики, міждисциплінарної співпраці, уваги до надійності результатів тощо;

осмислюючи перспективи генерального ШІ ("штучного інтелекту на рівні людини", *AGI*) фахівці зауважили, що сама ця ідея "надихнула багато фундаментальних досягнень", але з іншого боку, "успіх у створенні AGI може створити суспільство збоїв і ризиків… значних викликів безпеці", у тому числі — виклики для процвітання та виживання людства;

важливим є збереження різноманіття методологічних підходів до розвитку ШІ, використання старих парадигм (не нейронних) і новітніх, як і їх поєднання заради інновацій та подолання існуючих обмежень. Важливим є "врахування точок зору соціологів, етиків та політиків, для забезпечення відповідального та етичного розвитку та розгортання технологій ШІ, оскільки вже сьогодні стало зрозумілим, що ШІ — "це не просто інженерна дисципліна, а суспільна сила, яка змінює форму управління, культури, економіки та етики, що вимагає цілісного підходу до відповідальної розробки та впровадження".

Оцінюючи майбутні перспективи ШІ, фахівці звернули увагу, що сучасний ШІ нині значною мірою "керується приватним сектором", дослідження у сфері ШІ "лежать за зачиненими дверима великих технологічних компаній", а університетам важко з ними конкурувати через ресурси — дані, обчислення та зарплати — які мобілізуються приватним сектором. Тож їм потрібно віднайти своє місце і роль у новій ері "великого ШІ".

На початок 2025 р. ситуація, що склалася із ШІ як "кінцевим активатором" (у термінах М. Горовіца), підводить до таких висновків:

С вважається "більшим регулятором і меншим інноватором" у сфері ШІ та технологій, а інновації в технологіях впроваджуються, насамперед, США та деякою мірою — Китаєм, який "інновує ще трохи" [86];

Global AI Index, що охопив 83 держави свідчить, що лідери глобальної "гонки за ШІ" розглядають ШІ як стратегічну технологію для всіх сфер — від соціально-політичної, економічної, науково-технічної, культурної та ін.

до оборонної та безпекової, оскільки будь-які інновації в цивільній сфері, у державному управлінні можна використати для оптимізації сектору безпеки, оборони, розвідки, що й забезпечить державам-лідерам переваги, більшу чи меншу ефективність та, відповідно, конкурентоспроможність на міжнародній арені у ході асиметричних "гіпервоєн" (для "зламу" традицій, "забруднення" інфопростору, використання армії ботів для обробки мізків тих чи інших таргет-груп тощо). Однак, більша частина держав планети перебуває в аутсайдерах, тобто, ще не наблизилася до розробки і впровадження ШІ, або бере участь у зазначених процесах досить незначною мірою, або взагалі залишається на узбіччі прогресу і їхній потенціал замалий для врахування в рамках *Global AI Index*;

і демократії, і авторитаризми виявляють глибокий інтерес до ШІ. Але, враховуючи те, що демократія у планетарних масштабах деградує (найяскравіший приклад — руйнування демократичних інститутів Д. Трампом у США), то ШІ стане не лише інструментом процвітання та підвищення ефективності та конкурентоспроможності спільнот, але й чинником, який посилить спостереження, контроль (соціальний та політичний) за індивідами та соціумами, що обернеться обмеженням їхніх не лише свобод та прав, але й репресіями та цензуруванням слів, дій, вчинків, неконфіденційністю будь-яких персональних даних;

для наростаючої авторитарної хвилі ШІ може стати дієвим інструментом, який на певний час забезпечить ефективність високотехнологічних авторитарних режимів та аналогічних — централізованих — політичних систем, уможливить їхнє самозбереження у наскрізь контрольованому соціумі, де ризики для влади мінімізовані, а виклики будуть добре прогнозованими та ретельно заздалегідь прорахованими, що по-своєму забезпечуватиме авторитарним режимам і конкурентоспроможність на зовнішніх політичних та економічних ринках;

перевагам авторитаризму у розвитку ШІ сприяє байдужість щодо досягнення консенсусу при ухваленні рішень; відсутність чи ігнорування моральних чи етичних бар'єрів; обмеження соціальної та політичної участі (у ході обговорення, узгодження, пошуку компромісів і ухвалення рішень); здатність до швидкої мобілізації ресурсів (людських, фінансових, матеріальних та ін.); можливість ризикувати та залишатися поза межами підзвітності, громадського контролю, критики впродовж тривалого періоду перебування при владі чи в ієрархічній системі; невиконання зобов'язань та ігнорування вимог (інтересів індивідів, бізнесу) як в середині суспільств, так і міжнародних;

переваги демократії, такі, як приваблення наукових, експертних, прогнозних, бізнесових та інвестиційних талантів, створення умов (матеріальних, фінансових, обчислювальних тощо) як для вільного наукового пошуку, так і для функціонування вільних медіа як накопичувачів точних і різноманітних даних, що, врешті-решт, уможливлюють своєчасний і точний прогноз, готовність до міждержавної кооперації обертаються недоліками для авторитаризмів.

Розмірковуючи про геополітичні аспекти в контексті розвитку ШІ, фахівці уже відзначили [85] і те, що ШІ змінює динаміку глобальної влади та інвестиційні пріоритети націй, що впливають на економіку, безпеку, структури управління, і водночас ШІ створює проблеми для справедливості і контролю та стає "геополітичним полем битви", де країни змагаються за економічне, військове та стратегічне домінування, оскільки прагнуть використовувати штучний інтелект для отримання економічних, військових і стратегічних переваг, а це ускладнює міжнародне співробітництво.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. James V. Jeff Bezos is launching a new conference dedicated to AI, optimism, and Amazon. URL: https://www.theverge.com/2019/1/17/18186481/amazon-remars-jeff-bezos-conference-ai-machine-learning-robotics-space.
2. Allison G., Schmidt E. Is China Beating the U.S. to AI Supremacy? Belfer Center for Science and International Affairs. URL: https://www.belfercenter.org/publication/china-beating-us-ai-supremacy.
3. The Sam Altman drama points to a deeper split in the tech world. UTL: https://www.economist.com/business/2023/11/19/the-sam-altman-drama-points-to-a-deeper-split-in-the-tech-world?itm_source=parsely-api.
4. Святий Престол про можливості та ризики ШІ: не стати рабом машини. URL: https://www.vaticannews.va/uk/vatican-city/news/2025-01/svyatyj-prestol-pro-mozhlyvosti-ta-ryzyky-shi.html.
5. Wilkins A. 2023 was the year that artificial intelligence went mainstream. URL: https://www.newscientist.com/article/mg26034693-900-2023-was-the-year-that-artificial-intelligence-went-mainstream/.
6. Wilkins A. The shine began ro wear off AI in 2024 as advances slowed down. URL: https://www.newscientist.com/article/mg26435210-600-the-shine-began-to-wear-off-ai-in-2024-as-advances-slowed-down/.
7. Mollick E. Co-Intelligence: Living and Working with AI. Portfolio, 2024. 256 p.
8. Nickie L. Top 15 AI Trends for 2025: Expert Predictions You Need to Know. URL: https://techstartups.com/2025/01/01/top-15-ai-trends-for-2025-expert-predictions-you-need-to-know/.
9. Elon Musk`s DOGE working on a Custom chatbot called GSAi. URL: https://www.wired.com/story/doge-chatbot-ai-first-agenda/.
10. Li F.-F. The Worlds I See: Curiosity, Exploration, and Discovery at the Dawn of AI. Flatiron Books, 2023. 322 p.
11. Kiulian A. Why is AI English-Centric, and Why Is It a Very Big Problem? URL: https://www.linkedin.com/pulse/why-ai-english-centric-very-big-problem-artur-kiulian-gjsze/.
12. Кармазіна М. Інформаційні потоки: виклики для розвідки і суспільств у геополітичних реаліях сьогодення (аналіз дискурсів та практик. Геополітика потоків / монографія за ред. д. політ. н. Мироненка П. В., д. політ. н., про. Мокляка С. П. Київ : Видавництво Політія. С. 278—310.
13. Miailhe N. The geopolitics of artificial intelligence: the return of empires? *Politique étrangère*. 2018. № 3. С. 105—117. URL: https://www.cairn-int.info/abstract-E_PE_183_0105--the-geopolitics-of-artificial.html.

14. Professors in Print: “Digital Empires” by Anu Bradford. Columbia Law School. 2023. URL: https://www.youtube.com/watch?v=BMKbgbfK5r8.
15. Darroch R. What is the difference between national and international security? URL: https://www.quora.com/What-is-the-difference-between-national-and-international-security.
16. Routledge Handbook of the Future of Warfare / Edited by Artur Gruszczak, Sebastian Kaempf. 1st Edition. 2024. 490 p.
17. Годзинська І., Бондаренко А. 12 простих запитань про ШІ і майбутнє. Чи стане людина молодшим партнером штучного інтелекту? URL: https://texty.org.ua/articles/112522/12-pytan-pro-shi-i-majbutnye-rozmova-z-anatoliyem-bondarenkom-pro-zahrozy-shtuchnoho-intelektu/?src=read_next_banner&from=113389.
18. Hine E., Floridi L. Artificial intelligence with American values and Chinese characteristics: a comparative analysis of American and Chinese governmental AI policies. Ai & society. URL: https://doi.org/10.1007/s00146-022-01499-8.
19. Beraja M., Kao A., Yang D.Y., Yuchtman N. AI-tocratia. *The Quarterly Journal of Economics*, 2023. Volume 138, Issue 3. P. 1349–1402. https://doi.org/10.1093/qje/qjad012.
20. Hunter L. Y., Albert C., Rutland J., Topping K. Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. URL: https://www.researchgate.net/publication/378764079_Artificial_intelligence_and_information_warfare_in_major_power_states_how_the_US_China_and_Russia_are_using_artificial_intelligence_in_their_information_warfare_and_influence_operations.
21. Pauwels E. Preparing for Next-Generation Information Warfare with Generative AI. URL: https://www.cigionline.org/static/documents/Pauwels-Nov2024.pdf
22. Colon D. Le rôle de l’intelligence artificielle dans la guerre de l’information. *Revue Defence Nationale.* 2024. №873 P. 7–12. https://doi.org/10.3917/rdna.873.0007.
23. Moy W. R., Gradon K. T. Artificial intelligence in hybrid and information warfare. URL: https://www.taylorfrancis.com/reader/read-online/8c1d2f02-9b20-46bd-b660-3dd0b1b22740/chapter/pdf?context=ubx.
24. Ueno H. Artificial intelligence as dual-use technology. Research Outreach. URL: https://researchoutreach.org/community-content/artificial-intelligence-dual-use-technology/.
25. Ueno H. AI as a dual-use technology — a cautionary tale. URL: https://researchfeatures.com/ai-dual-use-technology-cautionary-tale/.
26. Krishnan A. Killer Robots legality and Ethicality of Autonomous Weapons. Routledge, 2009. 216 p.
27. Horowitz M. K. The Ethics & Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons. URL: https://direct.mit.edu/daed/article/145/4/25/27111/The-Ethics-amp-Morality-of-Robotic-Warfare.
28. Asaro P. Algorithms of violence: critical social perspectives on autonomous weapons. URL: https://doi.org/10.1353/sor.2019.0026.
29. McKay A., Watson A., Karlshoj-Pedersen M. Remote Warfare Interdisciplinary Perspectives. 2021. 265 p. URL: https://www.e-ir.info/wp-content/uploads/2021/01/Remote-Warfare-E-IR.pdf.
30. Bode I., Huelss H. Artificial Intelligence. Weapons Systems and Humen Control. URL: https://www.e-ir.info/2021/02/16/artificial-intelligence-weapons-systems-and-human-control/.

31. Goldfarb A., Lindsay J. R. Prediction and judgment. *International security*. 2022. V. 46. № 3. С. 1—10. URL: https://doi.org/10.1080/03071847.2019.1693803.
32. Buchanan B., Imbrie A. New fire: war, peace, and democracy in the age of AI. MIT Press, 2022. 344 p.
33. Human Rights Watch. Submission to the United Nations secretary-general on autonomous weapons systems. Human Rights Watch. URL: https://www.hrw.org/news/2024/05/06/submission-united-nations-secretary-general-autonomous-weapons-systems.
34. Filgueiras F. The politics of AI: democracy and authoritarianism in developing countries. Journal of information technology & politics. 2022. С. 1—16. URL: https://doi.org/10.1080/19331681.2021.2016543.
35. Scharre P. Four Battlegrounds: Power in the Age of Artificial Intelligence. W. W. Norton & Company, 2023. 496 p.
36. Allison G., Schmidt E. Is China Beating the U.S. to AI Supremacy? Belfer Center for Science and International Affairs. URL: https://www.belfercenter.org/publication/china-beating-us-ai-supremacy.
37. Zeng J. Artificial intelligence with Chinese characteristics. URL: https://dokumen.pub/artificial-intelligence-with-chinese-characteristics-national-strategy-security-and-authoritarian-governance-1st-ed-2022-9789811907210-97898119072279811907218.html.
38. Bryson J.J., Malikova H. Is there an AI Cold war? URL: https://online.ucpress.edu/gp/article/2/1/24803/117647/Is-There-an-AI-Cold-War.
39. World Artificial Intelligence Conference. URL: https://itpo-shanghai.unido.org/waic .
40. AI Superpowers: China, Silicon Valley, and the New World Order. Harper Business, 2018. 272 p.
41. The global democracy index: how did countries perform in 2024? URL: https://www.economist.com/interactive/democracy-index-2024
42. Щорічник СІПРІ 2024. Озброєння, роззброєння та міжнародна безпека. URL: https://www.sipri.org/sites/default/files/2024-08/yb24_summary_ukr.pdf.
43. 2025 Stockholm Forum on Peace and Development. URL: https://www.sipri.org/events/2025/2025-stockholm-forum-peace-and-development.
44. Farge E. China leading generative AI patents race, UN report says. URL: https://www.reuters.com/technology/artificial-intelligence/china-leading-generative-ai-patents-race-un-report-says-2024-07-03/.
45. Сааков В., Лебедєва О. Найдорожчою компанією в світі стала американська Nvidia. URL: https://www.dw.com/uk/najdorozcou-kompanieu-v-sviti-stala-amerikanska-nvidia/a-69417929.
46. Shepard M. The 10 most influential companies AI. URL: https://blog.acer.com/en/discussion/2252/the-10-most-influential-ai-companies.
47. Law M. Top-10: AI Companies to Watch. URL: https://aimagazine.com/top10/top-10-ai-companies-to-watch.
48. Glossary of artificial intelligence terms. URL: https://www.brookings.edu/articles/glossary-of-artificial-intelligence-terms/.
49. Ryall J. Japan under pressure to join campaign against killer robots. URL: https://www.dw.com/en/japan-under-pressure-to-join-campaign-against-killer-robots/a-50370333.
50. Connor R. Austria wants ethical rules for killer robots. URL: https://www.dw.com/en/austria-wants-ethical-rules-on-battlefield-killer-robots/a-55610965.

51. Maintaining American Leadership in Artificial Intelligence. URL: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.
52. US Senate AI 'Insight Forum' Tracker. URL: https://www.techpolicy.press/us-senate-ai-insight-forum-tracker/.
53. David E. Biden releases AI executive order directing agencies to develop safety guidelines. URL: https://www.theverge.com/2023/10/30/23914507/biden-ai-executive-order-regulation-standards.
54. Шварц Д. В ЄС узгодили регулювання штучного інтелекту. URL: https://www.dw.com/uk/v-es-uzgodili-reguluvanna-stucnogo-intelektu/a-67676239.
55. McCallum SH., Liv McMahon L., Singleton T. MEPs approve world's first comprehensive AI law. URL: https://www.bbc.com/news/technology-68546450.
56. Regulayion (EU) 2024/1689 of the European parliament and of the council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
57. A pro-innovation approach to AI regulation. URL: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.
58. McMahon L., Kleinman Z. AI Safety: UK and US sign landmark agreement URL: https://www.bbc.com/news/technology-68675654.
59. FACT SHEET: U.S. Department of Commerce & U.S. Department of State Launch the International Network of AI Safety Institutes at Inaugural Convening in San Francisco. URL: https://www.commerce.gov/news/fact-sheets/2024/11/fact-sheet-us-department-commerce-us-department-state-launch-international.
60. Connor R. China opts out of blueprint on military AI use. URL: https://www.dw.com/en/china-opts-out-of-blueprint-on-military-ai-use/a-70180690.
61. AI Safety in China: 2024 in Review. URL: https://aisafetychina.substack.com/p/ai-safety-in-china-2024-in-review.
62. Tobey D., Carr A., Bigg C., Fulton S., Ge A., Hoffner K. China releases AI safety governance framework. URL: https://www.dlapiper.com/en/insights/publications/2024/09/china-releases-ai-safety-governance-framework.
63. Freifeld K. US tightens its grip on AI chip flows across the globe. URL: https://www.reuters.com/technology/artificial-intelligence/us-tightens-its-grip-ai-chip-flows-across-globe-2025-01-13/.
64. Freifeld K. How the new AI chip rule from the US will work. URL: https://www.reuters.com/technology/artificial-intelligence/how-new-ai-chip-rule-us-will-work-2025-01-13/.
65. Вєнкіна К. США та Великобританія не підписали заяву щодо ШІ в Парижі. URL: https://www.dw.com/uk/ssa-ta-velikobritania-ne-pidpisali-zaavu-sodo-si-v-parizi/a-71577469.
66. McMahon L., Kleinman Z. UK and US refuse to sign international AI declaration. URL: https://www.bbc.com/news/articles/c8edn0n58gwo.
67. Делькер Я. Майбутнє ШІ: ЄС і США за Трампа обирають різні стратегії. URL: https://www.dw.com/uk/majbutne-stucnogo-intelektu-evrosouz-i-ssa-za-trampa-obiraut-rizni-strategii2-a-71490852/a-71490852.

68. Removing barriers to American leadership in artificial intelligance. URL: https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.
69. Public Comment Invited on Artificial Intelligence Action Plan. URL: https://www.whitehouse.gov/briefings-statements/2025/02/public-comment-invited-on-artificial-intelligence-action-plan/.
70. President Trump is Putting American Workers First — And Bringing Back American Manufacturing. URL: https://www.whitehouse.gov/articles/2025/03/president-trump-is-putting-american-workers-first-and-bringing-back-american-manufacturing/.
71. President Trump is Remaking America into a Manufacturing Superpower. URL: https://www.whitehouse.gov/articles/2025/03/president-trump-is-remaking-america-into-a-manufacturing-superpower/.
72. The China–U.S. Track II Dialogue on Artificial Intelligence and International Security Interim Report. URL: https://ciss.tsinghua.edu.cn/info/CISSReports/7041.
73. Policy of Artificial Intelligence Development in Poland. URL: https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F99995976.
74. Italian strategy for Artificial Intelligence. 2024–2026. URL: https://www.agid.gov.it/sites/agid/files/2024-07/Italian_strategy_for_artificial_intelligence_2024-2026.pdf.
75. Italian strategy for Artificial Intelligence. 2024–2026. URL: https://interoperable-europe.ec.europa.eu/collection/govtechconnect/news/italian-strategy-artificial-intelligence-2024-2026.
76. Festag S. Deutsche Unternehmen schlecht auf KI vorbereitet. URL: https://www.heise.de/news/Deutsche-Unternehmen-schlecht-auf-KI-vorbereitet-10185315.html.
77. Cisco AI Readiness Index. URL: https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/2024-m11/documents/cisco-ai-readiness-index.pdf.
78. Announcing The Stargate Project. URL: https://openai.com/index/announcing-the-stargate-project/.
79. KI als Markenzeichen für Deutschland. URL: https://www.bundesregierung.de/breg-de/service/archiv/ki-als-markenzeichen-fuer-deutschland-1549732.
80. Macron unveils plans for €109bn of AI investment in France. URL: https://www.ft.com/content/fc6a2d7a-5ed6-436e-84a5-dda86fc258d3.
81. The Rise of AI in Japan: A Complete Guide for 2025. URL: https://www.ulpa.jp/post/the-rise-of-ai-in-japan-a-complete-guide-for-2025.
82. South Korean AI Basic Law. URL: https://artificialintelligenceact.com/south-korean-ai-basic-law/.
83. Bendett S. The Role of AI in Russia's Confrontation with the West. URL: https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west.
84. The Global AI Index. URL: https://www.tortoisemedia.com/data/global-ai.
85. AAAI 2025 PRESIDENTIAL PANEL ON THE Future of AI Research. URL: https://aaai.org/wp-content/uploads/2025/03/AAAI-2025-PresPanel-Report-Digital-3.7.25.pdf.
86. Birchard R. How EU wants to change AI, big tech image amid US pressure. URL: https://www.dw.com/en/eu-big-tech-ai-regulation-innovation-jd-vance-v3/a-71577121.

РОЗДІЛ 4

ВЕПОНІЗАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ У XXI СТОЛІТТІ: ДОСВІД США

Ірина АЛЄКСЄЄНКО,
доктор політичних наук, професор

4.1. Штучний інтелект і національна безпека США

В умовах посилення значущості фактора військової сили, технології штучного інтелекту розглядаються як один із ключових інструментів зміцнення потенціалу мілітаризації. Відомо, що "на озброєння низки країн уже прийнято системи з елементами штучного інтелекту, починаючи з безпілотних літальних апаратів, роботів-вартових і закінчуючи системами обробки складної інформації" [12].

Погодимося з думкою дослідників про те, що сучасна гонка озброєнь здійснює новий виток, пов'язаний зі стрімким переходом в інформаційно-технологічну сферу, оскільки "в ситуації, коли протиборчі сторони мають ударні озброєння, які дають змогу кілька разів повністю знищити супротивника, змагатися далі в їхньому вдосконаленні не має сенсу" [13]. Семимильні кроки в розвитку цього комплексного міждисциплінарного науково-технологічного напряму сприяють тому, що на зміну перегонам ядерних озброєнь приходять перегони штучного інтелекту, переможець у яких, як передбачається, зможе забезпечити собі можливість глобального домінування в системі нового світового порядку, що народжується. Згідно з прогнозами аналітиків, незаперечна перевага лідера буде забезпечена тим, що "міць штучного інтелекту може блокувати будь-які інтелектуально-технологічні прориви інших центрів багатополярного світу, впливаючи, тим самим, на розвиток держав" [14]. У перспективах військового планування проглядаються виклики нової реальності, що формується. Наявність планів широкомасштабного впровадження штучного інтелекту в системи озброєнь і управління передових держав світу свідчить про те, що "у майбутніх збройних конфліктах у середньостроковій перспективі центр тяжіння зміститься на протиборство систем ШІ управління засобами ураження, прийняття рішень і розвідки" [15]. Кардинально трансформується уявлення про батальне мистецтво: передбачається, що в новій військовій парадигмі "застосування живої сили і наземних угруповань військ стануть не потенційною перевагою, а великим недоліком" [13]. Крім того, "застосування штучного інтелекту дасть змогу розірвати зв'язок між чисельністю населення і можливостями економіки держави, з одного боку, і боєздатністю збройних сил — з іншого" [10].

Сприйняття штучного інтелекту як цінного і ефективного інструменту військової могутності породжує не просто серйозну конкуренцію, а запекле суперництво між ключовими світовими центрами сили за досягнення

переваги в цій сфері. Умови наростаючої напруженості сучасного протистояння стимулюють безпрецедентне збільшення темпів науково-технічних розробок "інтелектуальної" зброї, її серійного промислового виробництва, випробувань і застосування на полі бою. Зокрема, документ під назвою "Інноваційна оборонна ініціатива США" містить план переходу до "Третьої стратегії компенсації (СК-3), покликаної забезпечити їхнє військове домінування у світі шляхом широкомасштабного використання штучного інтелекту в системах озброєнь" [11].

Також відомо, що в рамках реалізації концепції "Багатосферні операції" Пентагон нарощує зусилля у справі об'єднання інформаційних систем збройних сил США з метою забезпечення ефективного управління підрозділами, які перебувають у будь-якій точці світу. Передбачається, що застосування технологій штучного інтелекту надає можливість "мати інформаційну перевагу над противником під час воєнних дій шляхом скорочення часу на доведення інформації до необхідних споживачів, конкретних засобів ураження, оптимально розташованих по відношенню до об'єкта впливу, а також її використання в системі підтримки ухвалення рішень як бойових підрозділів, так і підрозділів по забезпеченню" [16].

Сучасна гонка озброєнь орієнтована на "перехід від автоматизації до інтелектуалізації, тобто впровадження високоінтелектуальних засобів збройної боротьби" [8]. При цьому, безсумнівно, імплементація цифрових платформ у системи озброєнь створює не тільки нові можливості, а й нові загрози. Стикаючись із проблемами непрозорості алгоритмів штучного інтелекту та загрозами неадекватного ухвалення рішень цифровим сервісом, необхідне повномасштабне усвідомлення ціни помилки. Однак протягом кількох останніх років уже понад чотири десятки держав (Велика Британія, Сполучені Штати Америки, російська федерація, Китай, Південна Корея, Ізраїль та ін.) активно долучилися до програми створення робототехнічних систем, що мають здатність вести бойові дії без безпосередньої людської участі [21]. Такі розробки можуть стати найпотужнішим каталізатором епохи наступного технологічного устрою, де головним орієнтиром проголошується створення систем сильного (загального) штучного інтелекту. Відмітимо, що "колискою" багатьох технологій була військова сфера, тому не можна виключати, що вже найближчим часом забезпечувати військову перевагу над противником будуть повністю автономні системи штучного інтелекту, що призведе до виникнення абсолютно нової конфігурації як на театрі воєнних дій, так і у військовому мистецтві взагалі.

Головна загроза переходу від роботизації до інтелектуалізації озброєнь і бойової техніки полягає у відстороненні людини від ухвалення рішень. Вихід за рамки чітко зрозумілих і заданих алгоритмів — це небезпека, яку не можна ігнорувати: "необхідно мати на увазі, що в умовах, коли технічним пристроям надано можливість давати оцінку розвитку подій під час воєнних конфліктів, існує ймовірність ненавмисного збільшення кількості незначних алгоритмічних збоїв, які здатні призвести до непередбачуваних і цілком

спровокованих з боку штучного інтелекту провалів стримування. При цьому, слід пам'ятати, що з моменту, коли обидві сторони конфлікту почнуть покладатися на штучний інтелект для управління поведінкою, самі системи почнуть взаємодіяти одна з одною унікальними (і непередбачуваними) способами" [22]. Це свідчить про необхідність і своєчасність фундаментального наукового розгляду питань розроблення та практичного впровадження нових систем озброєння і техніки з використанням ШІ. Ці застереження не безпідставні, так як сьогодні США, Китай, Великобританія, Франція, Ізраїль, Індія росія та низка інших країн реалізують національні військові програми, що передбачають застосування штучного інтелекту (ШІ) як у системах управління військами та зброєю, так і в окремих зразках озброєння та військової техніки (ОВТ). У загальному випадку під цим терміном можна розуміти здатність будь-якого штучно створеного об'єкта, наприклад, цифрової обчислювальної системи навчатися для вирішення певного класу завдань.

У дослідженні "Штучний інтелект і національна безпека", представленому на розгляд Конгресу США у 2019 року *(Artifi cial Intelligence and National Security - Congressional Research Service Report R45178 від 21.11.2019 року - AINS),* стверджувалося, що головною причиною створення різноманітних систем військового призначення, які володіють ШІ, є необхідність оперативного опрацювання структурованих і неструктурованих даних величезних обсягів (так званих великих даних), дана необхідність зумовлена постійним розширенням кількості, номенклатури та технічних можливостей сучасних засобів отримання інформації. Причому ці відомості можуть подаватися в різноманітній формі, включно з фото-, відео- і радіолокаційними зображеннями, а також аудіо- і текстовими повідомленнями різними мовами, даними, отриманими з кіберпростору, тощо. Там же зазначається, що ШІ в найближчому майбутньому поширіться в усіх видах бойової та забезпечувальної діяльності збройних сил (ЗС).

Згідно з прогнозом американської компанії "Markets and Markets Research", щорічне зростання світового ринку систем і засобів ШІ до 2027 року становитиме близько 27,8%. Основну роль у цьому відіграватимуть США, а ключовими виробниками обладнання та програмного забезпечення стануть американські компанії "Локхід-Мартін", "Рейтеон", "Нортроп-Грумман", "IBM", "Дженерал дайнемікс", "Нвідіа", англійська компанія "БАЕ системз" і французька "Талес". Водночас згідно з "Планом розвитку систем штучного інтелекту в Китаї" 2017 року, до 2030 року КНР має стати світовим лідером у технології ШІ [17].

Основним способом реалізації технологій, які широко застосовують сьогодні, зокрема при створенні систем штучного інтелекту військового призначення, є штучна нейронна мережа (ШНМ), що являє собою набір окремих цифрових обчислювальних елементів — нейронів, зазвичай розташованих на декількох послідовних шарах мережі. При цьому вона не програмується у звичному сенсі цього слова, а навчається. Ця особливість — головна перевага інноваційних нейронних систем (ІНС) перед традиційними алгорит-

мами обчислень. У процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними і вихідними, а також виконувати узагальнення. Вона з високою ймовірністю зможе отримати коректний результат на підставі даних, яких не було в навчальній вибірці, неповних і/або "зашумлених", а також частково спотворених даних.

Аналіз закордонних досліджень з даної проблематики дає нам уявлення про широке коло завдань, для ефективного вирішення яких у ЗС доцільно використовувати системи з ШІ. Так, вказується, що подібні системи будуть найкориснішими в розвідувальній діяльності, а також під час ідентифікації об'єктів у процесі опрацювання відео- і фотоматеріалів, які отримують із засобів видової розвідки. Окрім того, під час навчання на нейронну мережу подають великий масив спеціально підготовлених зображень, необхідних об'єктів розвідки (наприклад, літальних апаратів, кораблів, різних видів зброї, фізичних осіб тощо), зроблених під різними кутами, освітленням і в різному оточенні. Нейромережа аналізує характерні ознаки зображення (лінії, їхні з'єднання, форми, колір, розмір тощо) і будує модель розпізнавання, що забезпечує ідентифікацію об'єктів із мінімально допустимим рівнем помилок. У ряді країн уже сьогодні існують зразки озброєнь, що реалізують описані можливості ШІ. Так, на початку 2020 року компанія "Рейтеон" оголосила про розгортання системи розвідки, спостереження і цілевказівки "Істар" *(ISTAR - Intelligence Surveillance Target Acquisition and Reconnaissance)* на літаках Великої Британії "Сентінел" [9].

Ця система забезпечена ШІ, що робить можливим:

виявлення наземних і морських об'єктів, що цікавлять, і спостереження за їхнім переміщенням;

формування карти місцевості контрольованих районів;

оцінювання оперативної ситуації шляхом контролю активності переміщення різних об'єктів.

Подібними можливостями володіють системи розвідки, спостереження і цілевказівки на базі безпілотного літального апарату (БПЛА) *MQ-4C* "Тритон", що стоїть на озброєнні ВМС США[19].

Іншими завданнями, покладеними на системи зі штучним інтелектом, є визначення типу виявленого радіосигналу і радіопередавального засобу, що його випромінює, при веденні радіоелектронної розвідки, розпізнавання та переведення з іноземної мови в несприятливих умовах акустичної обстановки, формування геопросторових відомостей із розрізнених неструктурованих геоданих, оцінка призначення та характеристик різних об'єктів за результатами їхнього спостереження, оброблення двовимірних зображень об'єктів для отримання тривимірних.

За програмою "Блейд" *(BLADE - Behavioral Learning for Adaptive Electronic Warfare System)*, що виконується для агентства перспективних досліджень Пентагону ДАРПА *(DARPA),* компанією "Локхід-Мартін" розробляється система радіоелектронної боротьби, призначена для автоматичного придушення засобів радіозв'язку противника з безперервною оцінкою її ефективності з

метою подолання можливих заходів протидії. Стверджується, що ШІ відіграє ключову роль у забезпеченні ефективності створюваної системи [11].

Важливою прикладною сферою застосування ІНС у військовій справі є кіберпростір. В *AINS* вказується, що ШІ є ключовим елементом, який забезпечує виконання найскладніших кібероперацій. Його алгоритми, реалізовані в штучній нейронній мережі, можуть автоматично визначати наявність загроз, оцінювати їхню небезпеку, модифікувати з метою захисту від них власне програмне забезпечення. За оцінкою фахівців ДАРПА, виконання всіх цих операцій вимірюється секундами, а не місяцями, що характерно для великого штату експертів у відповідних галузях їх використання. Потенційно кіберсистеми з ШІ здатні одночасно розв'язувати завдання кіберзахисту і кібернападу. Відомо про успішні експерименти, проведені китайською корпорацією "Тенцент" з метою несанкціонованого доступу до ШІ, що розпізнають різні об'єкти. [20]. Метою такого доступу є приховування або підміна об'єкта розпізнавання. Спеціально для захисту від подібного шкідливого впливу на нейронну мережу, що спричиняє помилки в її поведінці, у ДАРПА існують спеціальні програми "Гард" *(GARD –Guaranteeing AI Robustness against Deception)* із розроблення апаратно-програмних засобів, які забезпечують гарантовану стійкість систем із ШІ від спроб їхнього злому. Експертами з кібербезпеки пропонується використовувати методи шифрування кодів виконуваних в *AIC* програмах для захисту від кібернападу.

Перспективним напрямком використання систем зі штучним інтелектом є інформаційні операції. Вже сьогодні вони вміють формувати підроблені фото, аудіо-, відеоматеріали, вбудовуючи в них реальні елементи обстановки і реальних дійових осіб, створюють в Інтернеті неправдиві профілі вигаданих або реальних людей з підтримкою ретроспективи їхніх сімейних відносин, освіти, кар'єри, зв'язків, кредитної історії тощо. Ці технології можуть використовуватися для створення неправдивих, так званих фейкових новин у засобах масової інформації, розроблення легенд оперативним співробітникам, дискредитації певних осіб або їх шантажу. Відомий проєкт "Медіфор" *(MediFor — Media Forensics)* агенції ДАРПА з протидії подібним системам, спрямований на розкриття та документування фактів їх застосування [21]. Однак відомо, що інтелектуальні засоби створення неправдивої інформації також можуть мати здатність до навчання методам протидії і способам їх виявлення.

Найперспективнішим напрямком розвитку військових систем, що володіють штучним інтелектом є централізоване планування і координація проведення військових операцій різного масштабу в повітряному, космічному, кібер-, морському і наземному просторі. Закордонні військові експерти назвали подібні дії "багатосферним управлінням і контролем" *(Multi-Domain Command and Control — MDC)*. Шляхом збирання та опрацювання всієї доступної інформації, отриманої із різних джерел, пропонується створювати інтегроване джерело інформації, так звану глобальну оперативну картину, на основі якої командирам різного рівня автоматично пропонуватимуться

найефективніші варіанти дій для досягнення цілей операції. Відомо про розробку подібних систем в інтересах ВПС США компаніями "Локхід-Мартін" і "Харріс" [15].

Крім того, слід зазначити, що різні автоматизовані системи підтримки ухвалення рішень і комп'ютерного моделювання оперативної обстановки у ЗС розвинених країн широко застосовували з 70-х років минулого століття, але ці системи не мали можливості навчання і, відповідно, штучного інтелекту.

Одними з перших використовуваних на практиці військових засобів зі ШІ стали імітаційні тренажери, які застосовували для навчання операторів різних військових машин. Метою імітації було відтворення реальних умов бойової обстановки, наприклад, шляхом формування відповідного відео- і звукового контенту для завантаження на пристрої відображення інформації в процесі підготовки оператора і зміна цих умов у відповідь на його дії [6].

Наразі найбільш широко ШІ використовується у військовій логістиці ЗС США. Такі системи вже зараз застосовують для оцінки потенційних потреб у запчастинах, для визначення найбільш раціональних за часом виконання та вартістю способів їхньої доставки. Принцип їх роботи полягає в автоматичному аналізі технічних параметрів, які надсилають різноманітні датчики, розміщені у засобах озброєння, з метою визначення необхідності та обсягу обслуговування або ремонту військової техніки. Американські військові фахівці зазначають, що логістичні військові системи зі ШІ забезпечують ефективнішу організацію операцій за критеріями: кількість задоволених заявок/вартість логістичних операцій/тривалість їх проведення [4].

Традиційно технології зі штучним інтелектом широко застосовують в автономних бойових і забезпечувальних мобільних засобах, здатних діяти самостійно і продовжувати виконання завдання (або повертатися на задану позицію) у разі втрати зв'язку з центром управління. Відомими прикладами такої техніки є безпілотні літальні апарати (БПЛА), автономні наземні машини, надводні та підводні апарати різного призначення. Ця сфера застосування ШІ добре опрацьована в теоретичному і прикладному плані завдяки наявності багатого досвіду використання подібних систем цивільного призначення. У військовій галузі відомий досвід застосування у ВПС США безпілотних винищувачів F-16 [13].

Прикладом сучасного ударного БПЛА є розроблений американською компанією "Кратос дефенс енд сек'юріті слюшинс" БПЛА XQ-58 "Валькірія". Відомо про відносно успішні випробування цього апарата, які були проведені у 2019 і 2020 роках. Даний БПЛА позиціонується як "напарник" керованого людиною винищувача. У ВМС США автономні системи зі штучним інтелектом тестують для вирішення завдань протичовнової та протидиверсійної оборони, контролю акваторії, прилеглої до важливих об'єктів берегової інфраструктури, доставлення необхідного спорядження на мобільні та стаціонарні морські об'єкти [7]. Також розробляються безлюдні підводні апарати великої водотоннажності типу "Лдуув" *(LDUUV — Large Displacement Unmanned Underwater Vehicle)* з автономністю ходу щонайменше 70 діб,

здатні самостійно розв'язувати навігаційні задачі, оминати різноманітні перешкоди та ідентифікувати підводні й надводні цілі.

Перспективним напрямком подальшого вдосконалення автономних транспортних і бойових засобів є забезпечення можливості їхньої автоматичної групової взаємодії. Так ДАРПА реалізує програми з відпрацювання питань групового застосування безпілотних літальних апаратів (до кількох сотень в одній групі), автономних надводних і підводних об'єктів, наземних мобільних роботизованих платформ різного призначення [25].

При цьому до автономних засобів групового застосування висуваються такі вимоги:

здатність визначати особливості навколишнього оточення, зокрема, встановлювати наявність інших учасників групи;

здатність автоматично організовувати канали зв'язку і визначати старшого групи або обирати нового при втраті попереднього;

здатність взаємодіяти для виконання поставленого завдання.

Згідно із заявами офіційних представників міністерства оборони КНР, восени 2020 року в Китаї вперше проведено успішну перевірку одночасного застосування 200 БПЛА, що взаємодіють між собою, для розв'язання завдань пошуку і знищення наземних цілей [3].

Крім того, ШІ може застосовуватися в таких військових галузях:

системи протиракетної та протиповітряної оборони, що використовують ШІ для формування інформаційно-розрахункових завдань у масштабі реального часу з урахуванням динамічно мінливої повітряно-космічної обстановки;

військові системи зв'язку, що використовують ШІ для вибору оптимальних каналів передавання інформації, використовуваних сигнально-кодових конструкцій, способів стиснення і закриття переданих повідомлень;

інтелектуальні боєприпаси, здатні самостійно ідентифікувати цілі та коригувати траєкторію під час підльоту до них;

приціли та пристрої відображення оптико-електронної інформації — від лобового скла на різноманітних машинах і до спеціальних шоломів та окулярів, які дають змогу формувати так звану віртуальну реальність, тобто, поєднувати в полі зору візуальні та цифрові зображення, які отримують від різних датчиків;

системи біометричної ідентифікації персоналу з метою визначення прав допуску до інформації, до приміщень, до управління зброєю тощо;

апаратура визначення стану військовослужбовців у військовій медицині із зазначенням переліку заходів щодо відновлення здоров'я;

метеорологічні системи, які оцінюють вплив погодних факторів на планування військових операцій [16].

Очевидно, що кількість напрямів і способів застосування штучного інтелекту у військовій справі буде тільки розширюватися слідом за появою нових ідей і технологій, що їх реалізують. Водночас слід відмітити основні проблеми, що впливають на ефективність і доцільність застосування штучного інтелекту.

По-перше, численні дослідження та експертні оцінки свідчать про неприпустимість повної довіри системам з ШІ в питаннях самостійного застосування зброї. Висловлюються побоювання, що ШІ потенційно здатний виробити рішення на нанесення випереджувального удару по цілях противника, якщо він побачить можливість отримання переваги в результаті такого удару. У дослідженні, проведеному американською організацією "Ренд корпорейшн", наголошується на небезпеці використання ШІ для ухвалення стратегічних військових рішень через відсутність критичного мислення в системах, які володіють ШІ, та їх схильності до змагальності, що може призвести до неправильного оцінювання ситуації [12].

По-друге, використання штучного інтелекту в автономних системах летальної зброї *(Lethal Autonomous Weapon Systems - LAWS)* виявляється вкрай чутливим до людської моралі. Під терміном "автономність" тут розуміється можливість ухвалення рішення на застосування зброї без участі людини-оператора.

З 2017 року в ЗС США ведуться роботи з інтеграції штучного інтелекту в чинні системи управління у рамках проєкту "Мейвен", є досвід застосування таких систем для виявлення та ураження цілей в Іраку, Афганістані та Сирії. В американських військових і науково-дослідних колах існують різні, часто протилежні точки зору на необхідність розвитку і використання автономних бойових засобів, що володіють ШІ [10]. Допускається застосування будь-яких форм електромагнітної або психологічної зброї та будь-якого руйнівного впливу на матеріальні об'єкти. Щодо автоматичного використання летальної зброї проти людини такої однозначності немає. Відомі приклади виходу компаній-розробників із відповідних програм через небажання брати участь у створенні бойових систем зі штучним інтелектом. Так, 2018 року компанія "Гугл" вийшла з проекту по створенню роботизованих бойових платформ у рамках проєкту "Мейвен". З іншого боку, вищі військові керівники США обґрунтовують необхідність розроблення таких систем як для пошуку і подолання їх вразливостей, так і через наявність подібних видів озброєння у противника.

Ще однією проблемою використання ШІ в системах військового призначення є його принципова вразливість для спеціалізованих атак на апаратно-програмне забезпечення. На відміну від традиційних кібератак, які вимагають для успішного здійснення наявності вразливостей апаратного і програмного забезпечення, викликаних, як правило, недостатнім опрацюванням питань безпеки при створенні або експлуатації такого забезпечення [9]. Атаки на ШІ в основному використовують вроджені обмеження, властиві таким системам. Під цим розуміється принципова неможливість на рівні звичайної, спеціально не підготовленої до конкретного виду атак системи, що володіє штучним інтелектом, відокремлювати реальні вхідні дані від фальсифікованих. Навіть для сучасних, математично вкрай складних алгоритмів реалізації ШІ, які практично ідеально працюють у нормальних умовах, незначна, невизначена для людського сприйняття, але продумана зміна вхідних

даних (наприклад, корекція зображення) може призводити до хибного результату обробки. Оскільки значення штучного інтелекту у військовій сфері визначається саме високою швидкістю опрацювання великих масивів різнорідних даних, що дає змогу істотно скорочувати тривалість циклу управління військами та зброєю, то зворотним боком такого процесу може виявитися катастрофічне погіршення ситуації в разі ухвалення рішень за неповними, невірними або, сфальсифікованими вихідними даними [24].

Таким чином, зарубіжні військові та науково-технічні фахівці здебільшого відзначають постійно зростаючий вплив штучного інтелекту на сучасні види ОВТ, який серйозно розширює їх можливості і змінює існуючі концепції їх використання в майбутніх війнах. Наприклад, у "Стратегії національної оборони" США йдеться про те, що ШІ "змінить суспільство і зрештою характер війни", а британський аналітик Дж. Джонсон стверджує, що "штучний інтелект може принести фундаментальні зміни у військову силу і спричинити наслідки у вигляді переформатування балансу сил. Перегони в розробці потенціалу ШІ безперечно вплинуть, зокрема, на геополітичне суперництво між Китаєм і США". Майбутні зміни пов'язують із підвищенням ефективності ведення військових операцій за рахунок значного поліпшення показників оперативності та точності застосування зброї, мінімізації помилок, спричинених людським чинником під час планування та здійснення бойових дій, оптимізації логістичних процесів у мирний і воєнний час. При цьому висловлюється побоювання, що справжні можливості ворожих систем озброєння, що володіють ШІ, можуть бути недооцінені аж до отримання результатів їх реального бойового застосування. У зв'язку з цим, згідно зі "Стратегією штучного інтелекту", що є однією зі складових частин "Стратегії національної оборони", МО США підтримуватиме випереджальний щодо держав-суперниць, насамперед росії та Китаю, темп розвитку та впровадження технологій штучного інтелекту з метою забезпечення стійкої переваги американських оборонних і наступальних систем озброєння над системами країн-суперниць [8].

Масштаб прийдешнього перетворювального впливу цифрових платформ на військову сферу настільки великий, що сьогодні це важко навіть собі уявити. Ситуація, що склалася, демонструє важливість інтенсивного, ретельного і всебічного вивчення цих технологій з метою використання їхніх переваг, а також нагальну необхідність виявлення потенційних небезпек, які випливають від них. Як це часто трапляється у сфері нових технологій, користь від їх застосування формулюється дуже чітко і виразно. Набагато складніше буває передбачити можливі ризики.

Отже, впровадження нових технологічних рішень, ризики мілітаризації штучного інтелекту перетинаються з побоюваннями щодо невизначеності перед онтологічною невідомістю майбутнього, усвідомлення яких багаторазово зростає на сучасному етапі, в часи геополітичних криз і соціальної нестабільності. Масштаби та реальні загрози сучасного інноваційного процесу в умовах безпрецедентного загострення міждержавних відносин і

наростання військового протистояння ставлять світову спільноту перед нагальною необхідністю пошуків здорового глузду і визнання пріоритетності розроблення нових глобальних підходів до розв'язання завдань гарантування безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Extradition To and From the United States: Overview of the Law and Contemporary Treaties. Congressional Research Service. 2016. 4 October. URL: https://crsreports.congress.gov/product/pdf/RL/98-958#page=39&zoom=auto,-457.
2. Tucker P. Russian Arms Production Slowed by Coronavirus, Analysts Find . Defense One. 2020. May 1. URL: https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/16507.
3. 10 U.S. Code 467 — Definitions. Legal Information Institute of Cornell Law School. URL: https://www.law.cornell.edu/uscode/text/10.
4. WSJ: исследователи из США следили за военными объектами в россии с помощью мобильников. ИноТВ. 2020. 19 июля. URL: https://russian.rt.com/inotv/2020-07-19/WSJ-issledovateli-iz-SSHA-sledili.
5. Machine Learning. The Next Wave. Vol. 22. No. 1. 2018. URL: https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-22-1.
6. Machine Learning. The Next Wave. Vol. 22. No. 2. 2019. URL: https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW_22-2.
7. The AIM Initiative. A strategy for augmenting intelligence using machines. Office of the Director of National Intelligence. 2019. 16 January. URL: https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf
8. Maintaining American Leadership in Artificial Intelligence: Executive Order 13859 of February 11. 2019. Federal Register. URL: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.
9. Summary of the 2018 Department of Defense Artificial Intelligence Strategy. U.S. Department of Defense. 2019. 12 February. URL: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.
10. H.R.1540 — National Defense Authorization Act for Fiscal Year 2012. SEC. 4601. The official website for U.S. federal legislative information Congress.gov. URL: https://www.congress.gov/bill/112th-congress/house-bill/1540/text/
11. H.R.4310 — National Defense Authorization Act for Fiscal Year 2013. SEC. 4601. URL: https://www.congress.gov/bill/112th-congress/house-bill/4310/text.
12. H.R.3304 — National Defense Authorization Act for Fiscal Year 2014. SEC. 4601. URL: https://www.congress.gov/bill/113th-congress/house-bill/3304/text.
13. S.1356 — National Defense Authorization Act for Fiscal Year 2016. SEC. 2404. URL: https://www.congress.gov/bill/114th-congress/senate-bill/1356/text.
14. In-Q-Tel: A New Partnership Between the CIA and the Private Sector . Central Intelligence Agency. URL: https://www.cia.gov/library/publications/intelligence-history/in-q-tel.

15. S.1790 — National Defense Authorization Act for Fiscal Year 2020. Congress.gov. URL: https://www.congress.gov/bill/116th-congress/senate-bill/1790/text.
16. National Intelligence Strategy of the United States of America . Office of the Director of National Intelligence. 2019. 22 January 2019. URL: https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.
17. National Counterintelligence Strategy of the United States of America2020-2022. URL: https://www.dni.gov/files/NCSC/documents/features/20200205National_CI_Strategy_2020_2022.
18. NCSC Unveils the National Counterintelligence Strategy of the U.S. 2020-2022. Office of the Director of National Intelligence. 2020. 13 February. URL: https://www.dni.gov/files/NCSC/documents/features/20200207National_CI_Strategy_Press_Release.
19. H.R.5515 — John S. McCain National Defense Authorization Act for Fiscal Year 2019. Sec. 1051. Congress.gov. URL: https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
20. Interim Report. National Security Commission on Artificial Intelligence. 2019. November. URL: https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view.
21. H.R.6395 — National Defense Authorization Act for Fiscal Year 2021. SEC. 1299C. Congress.gov. URL: https://www.congress.gov/bill/116th-congress/house-bill/6395/text.
22. Final Report. National Security Commission on Artificial Intelligence. 2021. March. URL: https://reports.nscai.gov/final-report/table-of-contents
23. Draft Final Report. National Security Commission on Artificial Intelligence. 2021. 19 January. URL: https://drive.google.com/file/d/1XT1-vygq8TNwP3I-ljMkP9_MqYh-ycAk/view.
24. Kegelmeyer W.P. 2019. Adversarial issues in machine learning. The Next Wave. Vol. 22. No. 2. P. 10-14. URL: https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW_22-2.
25. Whyte C. 2020. Problems of Poison: New Paradigms and "Agreed" Competition in the Era of AI-Enabled Cyber Operations // 20/20 Vision: The Next Decade / The NATO Cooperative Cyber Defence Centre of Excellence. 2020. P. 2015-2032. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.

4.2. Особливості використання технологій ШІ в розвідувальній діяльності: досвід США

Розвідка за своєю природою є винятково динамічним видом діяльності, завжди реагує на зміну зовнішньополітичного середовища, змінюючи тактику і перерозподіляючи спеціальні сили і засоби. Обмеження одних розвідувальних можливостей породжує необхідність розширення інших, на яких концентруються розвідувальні зусилля. Як показує аналіз закордонних джерел, особливо стрімко в сучасних умовах зростає роль технічної розвідки, зокрема радіоелектронної, телекомунікаційної та геопросторової, включаючи повітряну і космічну, які дають змогу не перетинаючи фізично кордонів

держави, яку розвідують, здобувати цінну інформацію, яка підлягає захисту 3. Використання ШІ-технологій у національних і наднаціональних засобах масової інформації (радіомовлення, супутникове телебачення, глобальна інформаційно-комунікаційна мережа Інтернет) багаторазово підвищує можливості деструктивного розвідувального впливу, спрямованого на розхитування конституційного ладу держави, яка є об'єктом розвідки, а також прямого матеріального підриву шляхом кібератак на службові ІТ-комунікації органів державного управління та об'єкти критичної інфраструктури.

У серпні 2016 р. американські спецслужби відстежували мобільні пристрої громадян росії, які їх зацікавили в силу свого службового становища використовуючи дані про геолокацію і тісні зв'язки розвідспільноти США з провідними ІТ-компаніями США, які допомогли визначати місця розташування пристроїв через управлінням операційними системами власного виробництва, яке було широко впроваджене компаніями у всьому світі. Тому для них не склало труднощів отримати інформацію про смартфони і їх власників, які регулярно відвідували певні місця земної кулі, де могло перебувати будь-яке військове відомство або військовий об'єкт. Якщо спецслужби візьмуть переміщення таких пристроїв по планеті на контроль, то деякі з них рано чи пізно можуть з'явитися на території країни, у якої зі США є договір про екстрадицію [2]. Тоді в один день невідомі люди в цивільному можуть поставити господарю такого пристрою кілька запитань і зробити пропозицію, від якої йому буде дуже складно відмовитися [3]. 2020 р. наочно продемонстрував, як ця схема працюватиме на практиці. У травні 2020 р. стало відомо, що приватна фірма "Орбітал інсайт" *(Orbital Insight)* проаналізувала вплив режиму самоізоляції, запроваджений в рф під час пандемії COVID-19 на роботу низки російських оборонних підприємств [4]. Аналітики компанії з використанням методів машинного навчання обробили анонімні телефонні дані, отримані від різних партнерів, та іншу інформацію з відкритих джерел. "Орбітал інсайт" — це не просто пересічна комерційна фірма: по-перше, вона займається аналізом геопросторової інформації *(geospatial analytics),* "яка ідентифікує географічне положення, кордони і характеристики природних або штучних об'єктів на землі" [5]; по-друге, членом її консультативної ради є Роберт Карділло *(Robert Cardillo),* колишній голова Національного агентства геопросторової розвідки США *(National Geospatial-Intelligence Agency)*, яка входить до американської розвідспільноти. Ці факти дозволяють зробити припущення про склад партнерів, які надали дані для аналізу.

У липні 2021 р. американські ЗМІ повідомили, що "група дослідників з Університету штату Міссісіпі" відстежувала мобільні телефони осіб, які відвідували російські урядові установи і військові обёєкти. Реалізація даного проєкту стала можливою через використання комерційного програмного забезпечення і зібраних пристроями та окремими додатками даних, зокрема про геолокацію на основі технологій ШІ. Фінансування проєкту забезпечили збройні сили США. Його метою була демонстрація сучасних можливостей зі збору та обробки даних з відкритих джерел з використанням ШІ [6].

Усе це стало можливим завдяки спрощенню доступу до даних завдяки розвитку та широкому впровадженню інформаційно-комунікаційних технологій і використанню методів машинного навчання, більше відомих як штучний інтелект (ШІ). Технології ШІ полягають в тому, що через алгоритм послідовно пропускають спеціальним чином підготовлені (розмічені) набори даних (тренувальні або навчальні дані) та підбирають певні внутрішні коефіцієнти так, щоб під час опрацювання перевірочних наборів даних система давала правильний результат. Якість системи на основі ШІ безпосередньо залежить, по-перше, від якості навчальних і тестових даних, а по-друге, від їх відповідності даним, з якими штучний інтелект працює на практиці.

У даному випадку мова йде про так званий "вузький ШІ", який являє собою алгоритм, заточений на розв'язання конкретної задачі, на кшталт розпізнавання облич або мови. Однак свою ефективність такі системи вже довели не раз.

Не дивно, що розвідспільнота США прийняла їх на озброєння. Такий інтерес до технологій ШІ розвідспільнота США демонструє постійно. Так протягом 2013–2019 років Агентство з національної безпеки *(National Security Agency)* США щорічно публікувало збірник матеріалів "Нова хвиля" *(The New Wave), який* включав наукові статті, що стосувалися однієї із інноваційних технологій. ШІ був його темою два роки поспіль — у 2018 і 2019 році. [7, 8].

На нашу думку цікавим і доречним в подальшому використання досвіду є питання розробки і впровадження механізму фінансування, який використовують спеціальні служб США до впровадження технологій ШІ. У цьому аспекти нами проаналізовані лише непряі дані. Так у Стратегії розвідспільноти в розділі шодо розробки і використання технологій ШІ зазначалося, що фінансові ресурси розвідки скромні й не можуть зрівнятися з ресурсами військових. Однак там же вказувалося, що члени розвідспільноти мають доступ до результатів НДДКР, які проводяться в інтересах збройних сил США. Уцілому, відкриті дані дають змогу оцінити цілі, завдання та проблеми в цій галузі. Силові структури в рамках робіт зі ШІ активно співпрацюють із технологічними компаніями та науковими школами. Зі зрозумілих причин, подробиці не розкриваються або розкриваються неохоче. Однак очевидно, що політичне рішення про широке впровадження ШІ в розвідку США, як і у випадку збройних сил держави, ухвалено і реалізовується досить прискореними темпами.

Свою стратегію у сфері штучного інтелекту розвідспільнота ухвалила ще у січні 2019 року, це на місяць раніше, ніж президент Дональд Трамп підписав Указ про Державну стратегію США в цій сфері [10], а Міністерство оборони опублікувало у відкритому доступі стислий зміст власної стратегії в сфері впровадження технологій ШІ. Відмітимо, що документ "Цільова ініціатива: стратегія посилення інтелекту розвідки за допомогою ШІ" не містить категорії "штучний інтелект", але відображає зміст інтересу розвідспільноти до даних технологій [9]. Він полягає у взаємному доповненні здібностей людини та обчислювальної техніки в галузі аналізу даних і, як наслідок, у

комплексному вилученні інформації з них. Штучний інтелект, автоматизація процесів і доповнення здібностей особового складу розвідслужб за допомогою технологій *(Artificial intelligence, process Automation, and IC officer Augmentation, AIM AAA technologies, AAA)* — це три кити, які, по розрахункам спецслужби США, виведуть інформаційно-аналітичне забезпечення процесу ухвалення рішень на якісно вищий рівень [5]. Уцілому підходи, завдання і проблеми розвідспільноти в галузі використання ШІ перегукуються з аналогічними завданнями, які впроваджує Міністерство оборони США (МО), а важливість цих технологій для спецслужб обґрунтовується у МО досить чітко: "Наші противники, особливо росія і Китай детально проаналізували потенціал ШІ для військових і розвідувальних операцій і активно фінансують процес розробки та впровадження технолоігій ШІ в цій сфері" [7].

Разом з тим, для повноцінного використання штучного інтелекту у своїх інтересах, розвідспільноті доведеться вирішити значну кількість завдань, які в Стратегії розділені на кілька категорій і для їх реалізації встановлено чіткі часові межі їх подолання з урахуванням пріоритетності та технічних можливостей.

Невідкладного розв'язання потребують завдання в таких галузях, як підготовка і використання даних; доступ розвідспільноти до обчислювальних потужностей; підвищення ефективності науково-технічної розвідки *(Science and Technical Intelligence)* у сфері ШІ; отримання фахівцями спецслужб глибокого розуміння особливостей і вразливостей цих технологій. На сьогодні бази даних — це та сировина для роботи ШІ, перероблюючи значні масиви якої він дає необхідний результат. Для навчання і перевірки якості роботи алгоритмів також потрібна величезна кількість даних, спеціальним чином відібраних і підготовлених. Причому вони мають бути того ж типу, як і ті, з якими системам доведеться працювати на практиці. У контексті завдань розвідспільноти це часто важко реалізувати. Тому Стратегія вимагає організувати всередині спільноти загальний доступ служб до навчальних і тестових наборів даних і до баз експертних знань, які містять неявні знання фахівців у розвідувальній сфері. Цікаво, що автори документу врахували існування конкуренції між службами і вжили привентивних заходів, попередивши всіх учасників про те, що дотримання заходів по захисту інформації не є підставою для "невиправданого обмеження" доступу до неї і її обміном всередині спільноти. Наявність інноваційних обчислювальних потужності є другою умовою, необхідною для реалізації та ефективного використання систем з технологіями ШІ. У зв'язку з цим Стратегія передбачає розвиток відповідної цифрової інфраструктури розвідспільноти *(IC Information Technology Enterprise)*, акцентиючи увагу на "завершенні формування системи високопродуктивних обчислювань", тобто створенні власних суперкомп'ютерів. Мова, йде про обчислювальні потужності, які створювалися у Форт-Міді *(Fort Meade),* де розташовані штаб-квартири Агентства з національної безпеки та Кіберкомандування США, враховуючи той факт, що в оборонному бюджеті США на 2012, 2013 і 2014 фінансові роки було схвалено фінансування за

темою “Центр високопродуктивних обчислень” у Форт-Мід. Кожного року у фінансовових документах фігурувала одна й та сама програма, але під різними назвами: у 2012 фінансовому році мова йшла про *High Performance Computing Capacity*; у 2013 фін. році — *High Performance Computing Center Inc 2*; у 2014 фін. році — *High Performance Computing Capacity Inc 3*, однак, очевидно, йдеться про три етапи робіт на одному й тому самому об’єкті. Варто також додати, що цей проєкт був передбачений законом про витрати на військове будівництво на 2012 фінансовий рік *(Military Construction Authorization Act for Fiscal Year 2012)*, а оборонний бюджет США на 2016 фінансовий рік був ухвалений з урахуванням розширення програми будівництва Центру високопродуктивних обчислень *(High Performance Computing Center*) у Форт-Міді, де були побудовані генерувальні потужності продуктивністю до 60 МВт для того, щоб забезпечити резервне джерело електроенергії для відповідного навантаження [12, 13, 14, 15].

З урахуванням побоювань у нарощування потужностей у розробці та використанні ШІ противником — росією і КНР, перед розвідспільнотою стоїть завдання посилити роботу по лінії науково-технічної розвідки *(S&TI)* для оцінки потенціалу в цій сфері іноземних держав і вжиття заходів з протидії технологіяним загрозам. Поставлені перед розвідкою США завдання на самих ранніх етапах роботи передбачали наявність фахово підготовленого особового складу. Слід зауважити, що в даному контексті розвідспільнота, як і інші держструктури, відчували критичний брак фахівців. Дефіцит кадрів настільки великий, що спецслужби побоюються навіть внутрішньої конкуренції за кваліфікованих співробітників.

Щодо стратегії впровадження технологій ШІ, відмітимо, що розвідспільнота працює над реалізацією завдання, щодо ухвалення рішень на основі “вузького ШІ”, як комерційними, так і з відкритим вихідним кодом. Однак Стратегія застерігає відомства від формального впровадження технологій ШІ і вимагає детальної оцінки процесів ефективності впроваджених систем і їх тісної кореляції з потребами спецслужб і їх стандартами у сфері безпеки і оборони, виходячи з того, що сучасний ШІ не досконалий і часто має проблеми не тільки з надійністю, кібербезпекою і доступністю у розумінні процесів. Варто відмітити, що самі розробники цих технологій не розуміють логіки навіть добре працюючого ШІ, та не можуть пояснити, чому система ухвалює те чи інше рішення. На їх думку проблема криється у фундаментальних принципах роботи самої технології.

Іншу небезпечну загрозу, яка характерна виключно для ШІ становлять так звані атаки з використанням змагального навчання *(adversarial learning, adversarial AI, adversarial ML).* Вони націлені на вразливості не в програмному або апаратному забезпеченні системи, а на особливості роботи самого алгоритму. Ідея полягає в тому, щоб через зміну (“отруєння”) навчальних, тестових і робочих наборів даних, створити у власника системи хибне враження про її якість роботи, або змусити систему видати потрібний зовнішнім атакувальникам результат. На думку фахівців таке втручання може мати

катастрофічні наслідки для ефективності системи. Тому на сьогодні цінність для спецслужб представляють не лише зібрані дані, а й алгоритми для їх опрацювання [8].

Небезпека змагальних методів ШІ *(adversarial AI techniques),* з точки зору спецслужб США, посилюється тим, що низка країн мають необхідні для їх застосування інструменти, набори даних і фахівців. Причому останні могли навчатися в тих самих університетах, що й американські фахівці. Усе це змушує США створювати методи і засоби забезпечення надійності систем зі ШІ та протидії будь-яким типам атак, включаючи проведення їхніх випробувань для виявлення можливостей і обмежень. Виявляється це дуже складне завдання, оскільки проблеми викликає навіть просте визначення контрольних показників *(benchmarks),* які дають змогу адекватно оцінювати успішність перебігу робіт зі створення системи і визначати її підсумкову якість. У разі комерційного програмного забезпечення Стратегією передбачений алгоритм його допуску до експлуатації в інтересах розвідспільноти, зокрема в закритих мережах. Загальнодоступні рішення зі ШІ передбачається допрацьовувати під конкретні потреби служб.

Використовуючи досвід військових відомств, які створили Об'єднаний центр штучного інтелекту *(Joint Artificial Intelligence Center, JAIC),* розвідспільнота заснувала свою спеціальну організацію *(AIM Center).* Її штат укомплектований фахівцями в галузі ШІ та машинного навчання з розвідспільноти та ІТ-індустрії. Організація налагоджує співпрацю з такими структурами, як Агентство перспективних досліджень у сфері розвідки, Управління перспективних досліджень Міністерства оборони, створеній за підтримки ЦРУ венчурною компанією "In-Q-Tel" [16], національною лабораторією Міністерства енергетики, Експериментальним відділ з оборонних інновацій МО *(Defense Innovation Unit-Experimental, DIUx)* та низькою комерційних компаній.

Сьогодні основна мета розвідспільноти США полягає в отриманні технічних засобів, які здатні обробляти різнотипні і розрізнені дані і виявляти взаємозв'язки між ними. У довгостроковій перспективі спеціальні служби США мають намір фінансувати фундаментальні дослідження по створення "сильного ШІ", який здатний витягувати інформацію з неповних і мізерних даних, виходячи з їх контексту. Цікаво, що до цієї ж категорії віднесено розв'язання кадрових проблем розвідспільноти, розроблення нормативно-правової бази спецслужб у сфері використання ШІ, а також розв'язання проблеми виявлення діпфейків *(deepfake)* [14]. І якщо перші два завдання неможливо вирішити швидко через специфіку підготовки фахівців, яка через складність технологій повинна розпочинатися зі школи, то щодо проблеми виявлення діпфейків немає ясності в тому, чи можливо її вирішити в принципі. Під діпфейками *(deepfake або machine-manipulated media)* розуміють "аудіо-, відеозаписи та зображення, згенеровані або суттєво модифіковані з використанням методів ШІ" настільки якісно, що їх практично не відрізнити від справжніх. Метою їх створення в контексті зовнішньої та внутрішньої політики може

бути проведення операцій з дезінформації якісно іншого рівня, включаючи "спотворенням інформації про будь-яку подію, спотворенням слів або поведінки окремих осіб, або зображенням осіб, яких насправді не існує" [17]. Це явище викликає неабияке занепокоєння у розвідспільноти США, оскільки значно ускладнює завдання визначення автентичності аудіо-, відеоматеріалів і графічних зображень [9]. Вцілому розвідспільнота США усвідомлює, що їй складно змагатися з приватними компаніями та Міністерством оборони у сфері ШІ. Тому, щоб уникнути дублювання в розробці систем, воно має намір зосередитися головним чином на вирішенні своїх специфічних завдань, "куди приватний сектор інвестує неохоче". Водночас спецслужби, як і військові, мають намір організувати широку кооперацію і співпрацювати з іншими відомствами, ІТ-компаніями, університетами, федеральними науково-дослідними та дослідно-конструкторськими центрами МО *(DoD's federally funded research and development centers, FFRDCs),* національними лабораторіями та міжнародними партнерами. Вони потребують взаємного обміну даними з ІТ-індустрією та залучення кваліфікованих кадрів. Однак специфіка процедури держзакупівель знижує інтерес комерційних компаній до співпраці з держструктурами. Для виправлення цієї ситуації розвідспільнота США має намір змінити свій підхід до організації державно-приватного партнерства, зробивши його більш гнучким.

У сфері міжнародного співробітництва спецслужби США віддають пріоритет взаємодії з країнами, які входять до розвідувального альянсу "Five Eye". Цілі США у цьому випадку традиційно прагматичні. Вони передбачають:

1) розширення своїх можливостей по збору необхідних даних;

2) підвищення якості та кількості отриманих даних;

3) доступ до результатів їхнього опрацювання союзниками;

4) узгодження в рамках альянсу підходів до використання нових технологій і забезпечення сумісності різних ШІ-систем [1].

Автори Стратегії фактично визнають, що, незважаючи на розвиток у світі галузі штучного інтелекту, розвідспільнота не належним чином готова до впровадження таких технологій і їй потрібне проведення серйозної підготовчої роботи. Проте в ухваленій Стратегії прямо поставлено завдання впровадження ШІ у спеціальних службах, тому з 2019 р. учасники розвідспільноти почали включати її у свої власні стратегії. Серед них можна виокремити наступні:

1). Національна розвідувальна стратегія США 2019 р. *(The National Intelligence Strategy of the United States of America 2019)* [18];

2) Національна контррозвідувальна стратегія США на 2020–2022 рр. *(National Counterintelligence Strategy of the U.S. 2020-2022)* [19, 20]. Цікавим у даному контексті є аналіз позиції Конгресу США щодовпровадження технологій ШІ в силових структурах США. Відмітимо, що американські законодавці повністю підтримують ентузіазм силових відомств щодо використання технологій штучного інтелекту в інтересах "національної безпеки США". Це виражається в пріоритетному забезпеченні законодавчої та фінансової

підтримки такої діяльності, незважаючи на жодні міжпартійні розбіжності з інших питань. Так, відповідно до припису закону "Про оборонний бюджет" на 2019 фінансовий рік для оцінювання досягнень і визначення напрямів подальшого розвитку державних робіт у галузі ШІ було створено Комісію національної безпеки зі штучного інтелекту. Її завданнями був аналіз методів і засобів, необхідних для розвитку Сполученими Штатами таких технологій в інтересах національної безпеки. Оцінці підлягав широкий спектр питань: конкурентоспроможність США в цій сфері; засоби і методи, які використовують США для забезпечення своєї технологічної переваги в даній сфері; ситуація у світі з роботами і досягненнями у сфері ШІ; ризики, пов'язані з їхнім практичним використанням, включаючи проблеми правового регулювання технологій ШІ і їх кореляція з нормами міжнародного права; вплив технологій ШІ на розвиток та перебіг конфліктів; способи залучення фахівців зі ШІ ; а також етичні питання використання ШІ [21].

Аналізуючи Закон "Про оборонний бюджет" на 2020 фін. р. *(NDAA-2020)* [17], відмітимо, що у ньому велику увагу приділено питанням розвитку технологій ШІ та машинного навчання у США та світі, а також потенційним загрозам національній безпеці, пов'язаними з використанням технологій ШІ. Технічний прогрес, зокрема в галузі ШІ, буде тільки ускладнювати виявлення шахрайських акаунтів і матеріалів, які спотворюють уявлення про реальні події, відмічалося в документі. Серйозні побоювання у законодавців викликають згадані вище діпфейки, сам факт появи яких є прямим результатом використання ШІ. Дедалі важче буде виявляти "шкідливу поведінку" в соціальних мережах [19]. Відзначено існування проблеми захисту самого ШІ від атак, спрямованих на спотворення результатів його роботи. У зв'язку з цим закон "Про оборонний бюджет" 2020 р. містив низку приписів американським силовим структурам щодо реагування на ці виклики. Перед Національною розвідкою США в цьому контексті, стоять два важливих завдання: оцінка ситуації у світі та в самій державі. Законодавці акцентували увагу на: аналізі потенційного впливу дипфейків на національну безпеку; огляді наявних і потенційних методів їх використання іноземними державами; технічних можливостях останніх у цій сфері. Увага розвідспільноти знову акцентувалася на діяльності росії та КНР у цій сфері. Перед директором Національної розвідки були поставлені важливі завдання:у звітування про потенціал рф і КНР у сфері не тільки створення, а й виявлення дипфейків; опис їхньої діяльності в цьому напрямі; характеристика державних структур і структур обох країн, що співпрацюють із державою, які беруть участь у таких роботах [10].

Для оцінки власних можливостей директору Національної розвідки доручалося: проаналізувати основні ініціативи спецслужб у сфері ШІ, їхню відповідність згаданій Стратегії розвідспільноти, ступінь координації з роботами військових і практику використання комерційних технологій; підготувати огляд технологій для атрибуції та протидії використанню дипфейків, що можуть бути або вже розроблені та розгорнуті у США в інтересах дер-

жави. Документ мав містити опис діяльності розвідспільноти в цій сфері; для стимулювання таких досліджень та їх комерціалізації організувати через Агентство перспективних досліджень у сфері розвідки змагання серед розробників технологій автоматичного розпізнавання діпфейків.

На тлі згаданих заяв про необхідність активізації науково-технічної розвідки США наукова спільнота мала посилити захист особливо важливих досліджень у різних галузях науки і техніки. Це стосувалося робіт вишів, які отримують державне фінансування (у будь-яких обсягах і на будь-які цілі). Директор Національної розвідки підготував перелік іноземних суб'єктів, які в контексті таких досліджень становили шпигунську або іншу загрозу національній безпеці. Не дивно, що до списку могли потрапити держави, корпорації, некомерційні та комерційні організації, будь-які дочірні або афілійовані з ними структури. Обліку підлягали "будь-які відомі або прогнозовані спроби іноземних суб'єктів чинити тиск на зазначені виші, через обмеженням свободи слова, розповсюдження дезінформації, здійснення впливу на професорсько-викладацький склад, дослідників і студентів". Для протидії цим впливам спецслужбам доручалося організувати тісну співпрацю з вишами та розробити необхідні правові або адміністративні заходи щодо їх попередження та усунення. [17].

Таким чином йшлося про те, що американська держава має намір посилити контррозвідувальне забезпечення діяльності своїх наукових кіл і взяти їх діяльність під посилений контроль з боку спеціальних служб США. Разом з тим варто відмітити, що наукове співтовариство визнало існування потенційних загроз, і було готове до співпраці з розвідспільнотою, очікуючи від неї рекомендацій щодо забезпечення безпеки [16].

У оборонному бюджету на 2021 фінансовий рік містилися чіткі вказівки адресовані розвідспільноті по забезпеченню інформаційного супровіду низки завдань інших відомств. В контексті аналізованих процесів отримала нову редакцію стаття закону "Про оборону" 2019 року про створення "Ініціативи щодо захисту вчених, які працюють в інтересах національної безпеки, від неправомірного впливу та інших загроз безпеці". Сама ініціатива націлена на захист як інформації про технології та їх розробки, важливі для забезпечення національної безпеки США, так і відповідних фахівців. Вона стосується насамперед робіт в інтересах військових. Тому за її реалізацію відповідає Міністерство оборони разом з "академічними та іншими освітніми та науковими організаціями". Для цього відомство має підготувати два переліки, у роботі над якими МО сприятиме Національна розвідка. Перший — міститиме перелік академічних інститутів Китаю, росії та інших країн, якщо вони, на думку США, відповідають певним критеріям загрози національній безпеці США [5].

По-перше, якщо вони вже були помічені в "неправомірному передаванні технологій, крадіжці інтелектуальної власності, шпигунстві (зокрема з використанням кіберпростору)" в сфері досягнень науки і техніки, або якщо є ризик таких дій з їхнього боку.

По-друге, якщо вони підпорядковуються військовим або розвідувальним службам.

По-третє, якщо вони були «викриті у вербуванні іноземних громадян для передачі ними секретної інформації для просування робіт військових або розвідки» або "у спробах приховати зв'язок з ними окремої особи або організації" [7].

Другий перелік стосувався "іноземних програм підготовки кадрів *(foreign talent programs)*, які загрожують інтересам національної безпеки США". У цьому контексті розвідспільнота прямо не згадувалася, проте її представники увійшли до "відповідних державних відомств" *(appropriate Government agencies)*, які мають допомогти МО у вирішенні завдань. До нього були занесені програми, які "загрожують дослідженням, що фінансуються Міністерством оборони"; "сприяють або залучені до кібератаки, крадіжки, шпигунства, спроб отримати право власності або інструменти впливу на компанії, або втручаються у справи США іншим чином". Підставою для включення до переліку №2 могли стати й інші причини на розсуд міністра оборони.

Обидва документи були нетаємними, але мали секретні додатки. Закон вимагав від військових надавати їх оборонним комітетам Конгресу не рідше ніж раз на рік і публікувати на своєму загальнодоступному інтернет-сайті. Усе це свідчило про використання потенціалу розвідки США для захисту американської науки і національної безпеки держави вцілому.

Закон "Про оборонний бюджет" 2021 р. запровадив для координації всіх державних зусиль за цим напрямом Національну ініціативу в галузі ШІ *(National Artificial Intelligence Initiative).* Її завданням було забезпечення взаємного інформування цивільних держструктур, МО та розвідспільноти про заходи, що вживаються учасниками таких робіт [2].

Окрім цього, Ініціатива передбачала створення двох структур. Перша — це Національний консультативний комітет з ШІ *(National Artificial Intelligence Advisory Committee),* який консультував президента США та адміністрацію вказаної Ініціативи *(National Artificial Intelligence Initiative).* За його створення відповідало Міністерство торгівлі [9]. Друга — це Робоча група по забезпеченню необхідними ресурсами національних досліджень у галузі ШІ *(National AI Research Resource Task Force).* За неї відповідають Національний науковий фонд і Управління науково-технічної політики Білого дому *(Office of Science and Technology Policy)* [11]. Ініціатива передбачала, що в обох випадках до роботи залучатиметься Національна розвідка США.

У січні 2021 р. Комісія Національної безпеки зі штучного інтелекту представили початковий варіант підсумкового звіту, який містив основні висновки і рекомендації з приводу розбудови ШІ галузі у США. У березні 2021 року, згідно норм Закону "Про оборонний бюджет" на 2020 рік, було опубліковано кінцеву редакцію звіту *(Final Report).* Порівнюючи з попередньою редакцією, яка нараховувала 130 сторінок, кінцевий варіант документу був обсягом у 756 сторінок. Разом з проєктами текстів президентських указів і

законів він був доповнений детальним планом заходів, які Комісія рекомендувала здійснити для реалізації своїх рекомендацій. Аналіз Звіту свідчить про те, що Комісія провела титанічну роботу з оцінки всіх сфер створення і запровадження як ШІ, так і пов'язаних із ним технологій. Один із розділів був присвячений використанню ШІ виключно в інтересах національної розвідки США. Виходячи з тексту, відмітимо, що розвідувальна спільнота США активно використовує технології ШІ в сфері забезпечення національної безпеки, роблячи це набагато швидше і продуктивніше, від інших силових відомств США. На думку очільника розвідки США це відбувається тому, що завдання технологій ШІ збігаються із завданнями розвідки, оскільки полягають у зборі та обробці даних, обсяги яких унаслідок поширення інформаційних технологій зросли в геометричній прогресії, і цей процес триватиме довго. У зв'язку з цим традиційних способів обробки даних стає недостатньо. Звіт вимальовував яскраві перспективи майбутнього для країн — лідерів у сфері ШІ - технологій: "ШІ оброблятиме масиви даних, зібраних з усіх джерел, знаходитиме критичну інформацію, виступатиме у ролі перекладача, об'єднуватиме набори даних із різних галузей, виявлятиме кореляції та зв'язки, переспрямовуватиме ресурси та інформуватиме аналітиків і осіб, відповідальних за ухвалення рішень" [13].

Комісія акцентувала на необхідності вирішення державою амбітної задачі: досягти розвідувальною спільнотою у 2025 році готовності доширокого використання найсучасніших ШІ-технологій в своїй діяльності *(AI-Ready by 2025).* Передбачалося, що до цього моменту розвіка США длсягне стану, за якого "особовий склад членів розвідспільноти матиме необхідну підготовку та володітиме таким рівнем цифрової грамотності, який надасть їм доступ до цифрової інфраструктури *(IC Information Technology Environment)* і програмного забезпечення, що інтегрують ШІ в робочий процес відомств на всіх етапах роботи" [14].

Основна ідея впровадження ШІ-технологій в розвідспільноті описана в підсумковому звіті Комісії наступним чином: "Після завершення автоматизації робочого процесу за окремими видами діяльності, розвідувальній спільноті США необхідно об'єднати їх у єдиний безперервний цикл аналізу розрізнених і різнорідних даних, що надходять з усіх джерел, за допомогою єдиної архітектури аналітичних механізмів, які безперервно удосконалюються *(continually learning analytic engines)*". Взаємне доповнення здібностей людини і ШІ відкрило можливість виягнути з наявних даних таку інформацію, яку людина не здатна отримати самотужки. Це сформує надійну і високоточну платформу для прогнозування і аналізу можливих викликів і загроз для національної безпеки держави і перетвориться на новий стандарт збору і обробки інформації, а більшу частину аналітичної роботи необхідно закріпити за ШІ. [4].

Доречно згадати про те, що в чернетці фінального звіту все це було оформлено у вигляді мети, яка передбачала "повноцінне впровадження ШІ в розвідувальній спільноті до 2030 року" *(The Goal: AI-Enabled Intelligence*

by 2030) [5]. Однак, Комісія зрештою вирішила, що характер невирішених технічних проблем і ситуація в самих відомствах роблять імовірність досягнення цієї мети в зазначені терміни настільки низькою, що тимчасові рамки прибрали. Разом з тим Комісія рекомендувала максимально впроваджувати технології ШІ в усі процеси — від обов'язкового первинного опрацювання даних машинними засобами до поширення та опрацювання інформаційних матеріалів розвідспільноти без участі людини.

Передбачалося, що матеріали обов'язково повинні мати дві версії: для людини *(human-readable)* і для ШІ *(machine-readable).* Це кардинально змінювало не лише підходи до роботи, а й методи розвідки — перспективні системи «мають бути оптимізовані для збору та обробки даних за допомогою ШІ», а також це сприяло переходу розвідспільноти на стандартне та уніфіковане ПЗ.

Незважаючи на прогресивні зрушення у запровадженні розвідкою США технологій ШІ, у підсумковому звіті йшлося й про наявні серйозні перешкоди цьому процесу на рівні влади/регулюючих органів, політиків, бюджетування, обміну даними та технічних стандартів. Для виправлення ситуації Комісія рекомендувала провести низку організаційних змін і призначень, оскільки інновації в галузі національної безпеки потребують сильного лідерства і мотивації. [18].

Передбачалося: по — перше офіс директора Національної розвідки має створити Раду з управління ключовими ризиками в галузі IT-модернізації *(IT modernization Senior Risk Management Council)* спецслужб.

По-друге, директор з науки і технологій *(Director of Science and Technology)* ODNI має бути паралельно призначений на посаду головного технічного директора всієї розвідспільноти *(IC's Chief Technology Officer, CTO).* Він несе відповідальність за координацію всіх питань, пов'язаних із використанням технологій ШІ.

Для уникнення дублювання, забезпечення сумісності розвідувальної і військової систем, пропонувалося організувати швидкий і безпечний спосіб обміну даними між відомствами. Страх понести покарання за наслідки помилок роботи ШІ є головною (після бюрократичних перепон) перешкодою для впровадження цих технологій. Ніхто не хоче брати на себе відповідальність за помилки, які важко спрогнозувати, включаючи їх ймовірність, сферу прояву, характер і рівень їх небезпеки, не маючи інформації про можливість його мінімізації. Тому у Звіті Комісії можна знайти завуальовані обережні рекомендації для відомств, щодо знаходження балансу між рівнем можливого ризику від впровадження ШІ -технологій і ризиком втрати лідерства у сфері розробки та запровадження ШІ у розвідувальній діяльності і військовій сфері. Говорячи інакше, Комісія рекомендувала знизити вимоги до безпеки і надійності роботи систем на основі ШІ-технологій, щоб максимально швидко прийняти їх на озброєння.

Особливу увагу у Звіті відводилос активізації збору даних по лінії науково-технічної розвідки *(S&TI)* для точності прогнозу і оцінки потенціалу противника у даній сфері. Разом з тим, слід відмітити, що швидкому і

ефективному вирішенню даних завдань на заваді стояв брак спеціально підготовленого особового складу, функції якого передбачали аналіз баз даних. Для виправлення ситуації Комісія рекомендувала директору Національної розвідки взяти даний напрям на особистий контроль, а також призначити відповідального за збір розвідданих за новими технологіями *(Emerging Technology Collection Executive)* і ввести його у склад Національної ради з розвідки *(National Intelligence Council).* Практика довела, що вирішити проблему дефіциту кадрів було набагато складніше, ніж подолати бюрократію, через низку причин, джерелом яких були наступні процеси:

По-перше, термін підготовки технічних фахівців — це досить тривалий і складний процес, так як за висновками Комісії у США відмічено досить низьку якість освіти в галузі точних наук *(science, technology, engineering, and mathematics, STEM)* [3].

По-друге, ІТ-фахівці не дуже охоче йдуть працювати в держструктури, через те, що на держслужбі оплата нижча, ніж в ІТ-компаніях.

Щоб компенсувати це, у згаданому першому проміжному звіті Комісія рекомендувала пропагувати важливість держслужби та наголошувати на громадянській свідомості потенційних працівників, показуючи "привабливі способи зробити свій внесок у прогресивний розвиток суспільства, розв'язуючи винятково складні та важливі проблеми" [22]. Але з часом було з'ясовано, що різниця в оплати праці — це не головна причина. Перешкода крилася в бюрократичній тяганині, з якою стикаються ІТ- фахівці і яка не дозволяє вчасно використати доступний їм інструментарій, який через бюрократичні зволікання встигає застаріти, перш ніж вони отримають право використовувати його для роботи. При бажанні вступити на держслужбу фахівці стикаються з кадровим формалізмом у процесі оцінки відповідності кандидатів вимогам до посади, який подолати вдається далеко не всім претендентам [20]. Самі відомства не застосовують спеціальних механізмів найму, наприклад, право найму спеціалістів без конкурсу або організацію стажувань і стипендіальних програм.Через це у Звіті Комісія зазначила, що технічні фахівці в галузі ШІ становитимуть меншу частину загального персоналу розвідспільноти.

Але, не дивлячись на це, більша частина, що залишилася, все одно повинна розуміти основи, політику, функції та механізми застосування ШІ, щоб ефективно використовувати можливості ШІ технологій. І обов'язково потрібні керівники на всіх рівнях, які розуміють особливості розробки, використання, обмеження та сильні сторони ШІ. Крім того, для розуміння потенціалу особового складу службам рекомендувалося провести його оцінювання і створити систему заохочення за володіння навичками в галузі ІТ і ШІ-технологій.

Беручи до уваги всі переваги і недоліки, описані вище, можна зазначити, що на цьому фоні лідерами в галузі ШІ-технологій були і залишаються приватні компанії. Вони розвиваються швидше за держсектор через відсутність настільки жорстких вимог щодо безпеки та надійності систем. Через кращу оплату праці та технічну оснащеність є більш привабливим місцем роботи

для фахівців. Крім того, у разі витоку даних, або будь-яких інших проблем, дані структури завжди можуть відхреститися від них (за аналогією з втратами особового складу приватних військових компаній), вказавши, що вся вина лежить на підряднику, який не організував роботу належним чином. Можливо, остання обставина навіть є однією з ключових перешкод для впровадження ШІ в держструктурах.

Керівництво ж останніх і так все влаштовує, і в нього не виникає бажання проявити політичну волю для реального подолання решти проблем. У зв'язку з цим розвідспільнота завжди буде зацікавлена в залученні комерційних компаній для виконання своїх завдань, а підрядники не залишаться без персоналу і роботи. Слід відмітити, що ШІ-системи, які використовує розвідка США на основі відкритих джерел інформації дають змогу комерційним компаніям домагатися настільки серйозних результатів, що Комісія наполегливо рекомендувала спецслужбам максимально інтегрувати ці методи в сучасний робочий процес.

Таким чином, розвідспільнота разом зі збройними силами є головними державними споживачами технологій у сфері штучного інтелекту в США. Зараз вони стикаються з серйозними проблемами впровадження таких систем через нестачу фахівців, відсутність відповідної технічної інфраструктури та організаційних питань, включаючи велику інертність бюрократичної системи, що чинить опір будь-яким інноваціям.

Проте, керівництвом США поставлено завдання впровадити ШІ-технології в спеціальних службах. Конгрес, незважаючи на міжпартійні протиріччя, також не ставить під сумнів важливість його вирішення. Для виявлення проблем, перспектив і шляхів розвитку галузі було створено Комісію національної безпеки зі штучного інтелекту, у складі якої практично немає випадкових людей.

Переважна більшість її членів — це провідні фахівці з ШІ найбільших ІТ-компаній США. Донедавна очолював її Ерік Шмідт, людина, під керівництвом якої "Гугл" стала тією корпорацією, яку ми знаємо сьогодні, і той, хто одним із перших забив на сполох з приводу розвитку ШІ у світі та небезпеки для США упустити лідерство в цій сфері. Посаду його заступника обіймав Роберт Ворк, який, будучи заступником міністра оборони США, дав старт першій пілотній програмі використання ШІ у збройних силах. Комісія розгорнула активну роботу і за підсумками її діяльності було сформовано не формальний, а деталізований документ, що містив велику кількість детально розроблених заходів і законопроектів. У цьому видно явну зацікавленість учасників у реальному досягненні результату — широкому впровадженні ШІ на практиці, зокрема в розвідспільноті, незважаючи ні на який опір системи. Комісія підкреслювала, що "ШІ — це квінтесенція технологій подвійного призначення" [24] і запізнення в його впровадженні вкрай небезпечнедля національної безпеки США.

Однак у звіті простежується і прагнення пролобіювати інтереси ІТ-індустрії. Документ дає опис максимально успішного варіанту розвитку технологій, які навряд чи можуть залишити байдужим чиновників .

Разом з тим, визнаючи серйозні технічні та етичні проблеми впровадження та використання ШІ, Комісія рекомендувала суттєво знизити вимоги з безпеки до таких систем. Причому за відсутності конструктивних аргументів, вона використовує універсальний аргумент — інтереси національної безпеки США.

Отже, сьогодні в галузі ШІ відбувається зворотна конверсія: технології, доведені комерційними компаніями до готовності для практичного використання, ставляться на військово-розвідувальні рейки. Комісія висловила побоювання, щодо систематичного збіру даних про компанії, громадян і державні структури США, так як розгледіла в цьому процесі шпигунтво на основі ШІ-технологій, яке докорінно відрізняється від традиційного шпигунства, так як ШІ ускладнює приховування інформації про особисте фінансове становище, розпорядок дня, звички, стосунки, здоров'я і навіть емоції, тому паралельно необхідно розроблювати адекватні ШІ технологіям заходи щодо захисту інформації.

Нова проблема полягає в тому, що вразливості окремих громадян і приватних компаній стають викликами і загрозами національній безпеці держави, оскільки противник може отримати доступ до: характеристик людей і соціальних мереж, використати їх для провокування соціальної напруги; передбачити реакції людей на зовнішні впливи; і змоделювати варіанти маніпулювання поведінкою мас або заподіяння шкоди. Прогнозування і аналіз цих методів і є головним завданням розвідувальної спільноти держави в умовах вепонізації технологій ШІ.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Draft report on a European Parliament recommendation to the Council and the Vice- President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy … after the Russian invasion of Ukraine 2022/2039INI. European Parliament. URL: https://www.europarl.europa.eu/doceo/document/AFET-PR-730096_EN.
2. Bächle T. C., Bareis J. "Autonomous weapons" as a geopolitical signifier in a national power play: Analyzing AI imaginaries in Chinese and US military policies. Eur J Futures Res. 2022. N 10. P. 20—37.
3. Johnson J. Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis. 2019. P. 39—51.
4. Daniel Araya and Meg King.The Impact of Artificial Intelligence on Military Defence and Security. CIGI Papers. N 263. March 2022. P. 113—129.
5. Ananny M., Crawford K. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media & Society. 2018. Vol. 20. N 3. P. 973–989.
6. Hagendorff T. The Ethics of AI Ethics: An Evaluation of Guidelines // Minds & Machines. 2020. Vol. 30. P. 99—120.
7. Artificial Intelligence and National Security. November 21. 2019, Congressional Research Service. URL: https://fas.org/sgp/crs/natsec/R45178

8. Bächle T. C., Bareis J. Autonomous weapons» as a geopolitical signifier in a national power play: Analyzing AI imaginaries in Chinese and US military policies. Eur J Futures Res. 2022. N 10. P. 20–37.
9. Berryhill J., Heang K. K., Clogher R., McBride K. “Hello, World: Artificial intelligence and its use in the public sector”. OECD Working Papers on Public Governance. 2023.N 36. P.36–49.
10. Corrigan J. Three-Star General Wants AI in Every New Weapon System. November 2017. URL: https://www.defenseone.com/technology/2017/11/stargeneral-wants-artificial-intelligence-every-new-weapon-system/142239/.
11. Daniel Araya and Meg King.The Impact of Artificial Intelligence on Military Defence and Security // CIGI Papers. N 263. March 2022. P.60–79.
12. Defense Science Board. Summer Study on Autonomy. June 9. 2019. P. 12—19.
13. Hacker Ph., Petkova B. Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers.15 NW. J. TECH. & INTELL. PROP.1. 2020.P. 142—179.
14. Huizing A., Heiligers M., Dekker B., de Wit J., Cifola L., Harmanny R. Deep Learning for Classification of Mini-UAVs Using Micro-Doppler Spectrograms in Cognitive Radar. IEEE A&E Systems Magazine. 2021. N 10. P.59—72.
15. Johnson J. Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis. 2019. P.91—135.
16. Konaev M., Chahal H., Fedasiuk R., Huang T., Rahkovsky I. U. S. Military Investments in Autonomy and AI. Center for Security and Emerging Technology. October. 2020. P. 16—26.
17. Osborn K. Here Is the Army’s Hyper-Networked Vision of Future War. June 2. 2020. 157 p.
18. Ownby M., Dr. A. Kott. Reading the Mind of the Enemy: Predictive Analysis and Command Effectiveness. The State of the Art and The State of the Practice. 2021. P. 145.
19. Reese Hedberg S. DART: Revolutionizing Logistics Planning // IEEE Intelligent Systems. May/ June. 2022. P. 81–83.
20. Schubert J., Brynielsson J., Nilsson M., Svenmarck P. Artificial Intelligence for Decision Support in Command-and-Control Systems.23rd International Command and Control Research & Technology Symposium “Multi-Domain C2”.2021.239 p.
21. Spangler M. Nagorno-Karabakh Is Ready for Another War. 23. Szabadföld I. Artificial Intelligence in Military Application // Opportunities and Challenges, Land Forces Academy Review. 2021. Vol. XXVI. N 2 (102). P. 157—165.
22. Signals intelligence (SIGINT): What it is and why you should care. URL: https://prepperdavesonline.com/2022/01/09/signals-intelligence-sigint-what-it-is-and-why-you-should-care.
23. Secrecy reigns at the EU’s Intelligence Analysis Centre. URL: https://www.statewatch.org/media/docu- ments/analyses/no-223-eu-intcen.
24. Third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 Decem- ber 2016 and 5 December 2017. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.

ЧАСТИНА ІІ
ПРИКЛАДНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

РОЗДІЛ 5
ОСНОВИ ТА СКЛАДОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Юрій ЛИСЕЦЬКИЙ,
доктор технічних наук, доцент

5.1. Теоретичні та математичні основи штучного інтелекту

Штучний інтелект, як галузь дослідження була заснована на семінарі, проведеному у Дартмутському коледжі в США в 1956 року. Цей семінар мав важливе значення для науки: він об'єднав вчених, що цікавилися проблемою моделювання людського розуму, затвердив появу нової галузі науки і дав їй назву — artificial intelligence — штучний інтелект. Організаторами заходу були Джон Маккарті, Марвін Мінскі, Клод Шеннон і Натаніель Рочестер. Вони запросили всіх відомих американських дослідників, чия робота так чи інакше була пов'язана з питаннями теорії управління, теорії автоматів, нейронних мереж, теорії ігор і дослідженням інтелекту.

З початку 2000-х років зі стрімким розвитком інформаційних технологій ШІ починають дуже активно і широко використовувати, зокрема у інформаційної безпеки, з часом у кібербезпеці, а зараз і у кіберрозвідці. Тому в цьому контексті висвітлення теоретичних і математичних основ ШІ є доволі доцільним.

Наука про ШІ починає розвиватися з 40-х років минулого століття, коли група вчених з різних галузей прийшли до думки про можливість створення штучного мозку. Тоді почали формуватися його теоретичні та математичні основи [1]. Дослідження в галузі нейрології показали, що мозок являє собою мережу з нейронів, які обмінюються електричними сигналами за принципом "все або нічого", 0 або 1. Кібернетика американського математика Норберта Вінера описала основи управління і стабільності в електричних мережах [2]. З теорії інформації американського електротехніка і математика Клода Шеннона стало відомо про цифрові сигнали [3]. Англійський математик і криптограф Алан Тюринг теоретично обґрунтував можливість будь-яких обчислень за допомогою цифрових операцій [4]. Американський нейропсихолог і нейрофізіолог Уоррен Ма-Каллок та нейролінгвіст і математик Волтер Піттс проаналізували мережі, які складають з ідеалізованих штучних нейронів, і продемонстрували, як вони можуть виконувати найпростіші логічні функції [5]. Канадський фізіолог і нейропсихолог Дональд Гебб запропонував теорію навчання, засновану на кон'юнктурі нейронних мереж та синапсів, здатних з часом посилюватись чи слабшати [6]. Ці науковці були першими, хто описав те, що дослідники згодом назвуть нейронною мережею [7].

У 1957 році Френком Розенблаттом був запропонований Перцептрон (англ. perceptron) — математична або комп'ютерна модель сприйняття інформації мозком (кібернетична модель мозку), уперше втілена у вигляді електронної машини "Марк-1" у 1960 році. Перцептрон став однією з перших моделей нейромереж, а "Марк-1" — першим у світі нейрокомп'ютером [8].

Отже, нейромережа — це по суті математична модель, яка емулює роботу нервової системи людини. В свою чергу, математична модель — це система математичних співвідношень, які описують досліджуваний процес або явище [9]. Таким чином, нейромережа — це математична модель, яка описує математичними формулами взаємозалежності між різними факторами і дозволяє виявити закономірності взаємозалежності вхідних даних та кінцевого результату в процесі навчання. У математичній моделі нейромережі є вузли — штучні нейрони. Вузли з'єднані між собою зв'язками і передають сигнали один одному (рис. 5.1).

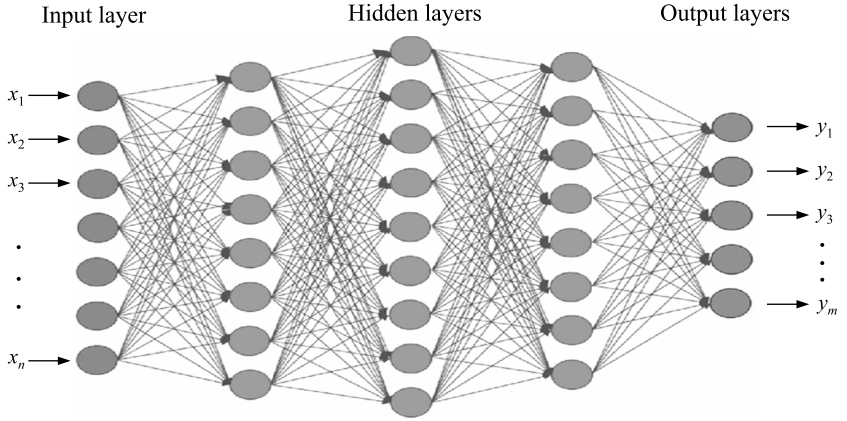


Рис. 5.1. Схема багатошарової нейронної мережі

Перцептрон (Perceptron) — це найпростіша математична модель нейрона [10]. Перцептрон можна візуалізувати, як представлено на рис.5.2:

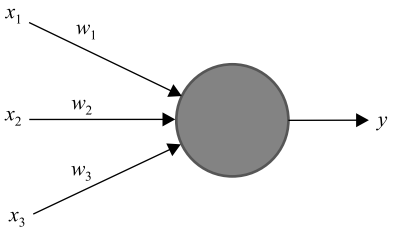


Рис. 5.2. Схематичне зображення перцептрону

Перцептрон — це математична функція, якій задається декілька параметрів *x,* а результатом обчислення є число *y*, наприклад *y = 3*x*. Кожному вхідному значенню «*x*» надається певна вага *w*, яку можна регулювати, в залежності від того, наскільки це значення важливе та впливає на результат обчислення. В даному випадку, ця функція буде виглядати так:

$$y = \begin{cases} 0, \text{ якщо } \Sigma_i w_j x_j \leq \text{порогове значення} \\ 1, \text{ якщо } \Sigma_i w_j x_j > \text{порогове значення} \end{cases}$$

Насправді функція виглядає складніше: по суті вона означає, що результат роботи нейрону є 0, якщо сума добутків всіх вхідних параметрів та їх вага менше певного порогового значення або дорівнює 1, якщо сума всіх вхідних параметрів та їх вага більше певного порогового значення. 0 — нейрон пасивний, 1 — нейрон активний. Результат обчислення передається як вхідний параметр іншим нейронам наступного шару нейромережі. Чим більше *y* — тим сильніше активується нейрон на наступному шарі і так далі.

Отже, роботу перцептрону можна уявити як пристрій, який приймає рішення на основі зважених вхідних даних. Якщо уявити, математичну модель з тисячею перцептронів, тобто тисячу нейронів у кожного на вході будуть тисячі чи десятки тисяч *x*. І чим більше вузлів, тим більшу варіативність може моделювати мережа. Керуючи вагою з'єднань між нейронами ми можемо підлаштовувати нейромережу, та таким чином навчати її видавати очікувані результати.

Перцептрон — це найменш ефективна модель вузла нейромережі. Крім перцептрону ще є лінійний нейрон, сигмоїдний нейрон, нейрон з функцією активації ReLU, нейрон з функцією активації tanh, нейрон з функцією активації softmax [11]. Кожен має специфічні функції для різних завдань нейромереж.

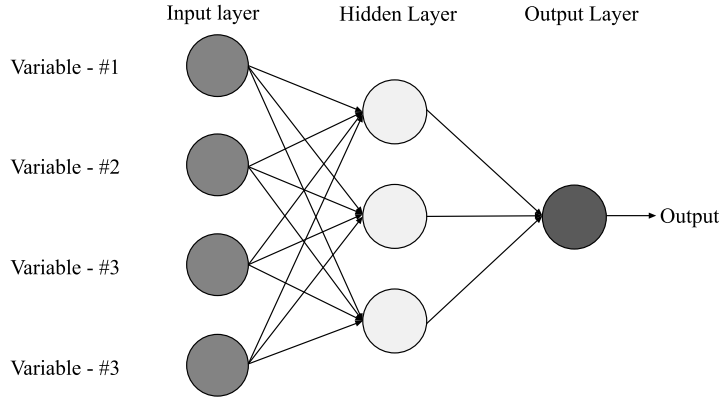
Архітектуру нейромережі можна поділити на дві складові: архітектуру математичної моделі нейромережі та архітектуру програмного забезпечення, яке реалізує функції нейромережі. Для початку наведемо найбільш використовувані архітектури математичних моделей:

Нейромережі прямого зв'язку (Feedforward). Сигнали передаються в одному напрямку від одного шару до іншого. Це найпростіша структура призначені для класифікації чи прогнозування (рис.5.3).

Нейромережі зі зворотнім зв'язком (Recurrent). У цій структурі нейрони можуть мати зв'язки не тільки в прямому, але й у звортньому, створюючи цикли в мережі (рис. 5.4). Використовується, наприклад, у машинному перекладі, де контекст та попередній контекст важливі для правильного перекладу.

Згорткові нейромережі (Convolutional). Дозволяють локальну обробку даних та розпізнавання властивостей в зображеннях. Згорткові нейромережі ефективні в розпізнаванні об'єктів та виявленні патернів в зображеннях (рис. 5.5).

Окрім вказаних, є рекурентні нейромережі з довготривалою пам'яттю (Long Short-Term Memory, LSTM), гортково-рекурентні нейромережі (Con-



An example of a Feed-forward Neural Network with one hidden layer (with 3 neurons)

Рис. 5.3. Feedforward neural network

Recurrent Neural Networks

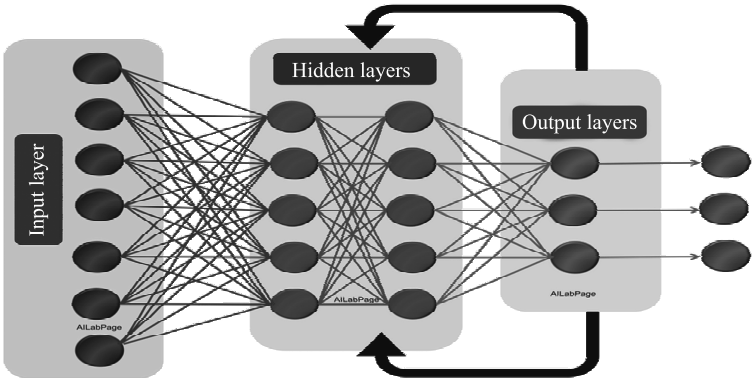


Рис. 5.4. Recurrent neural network

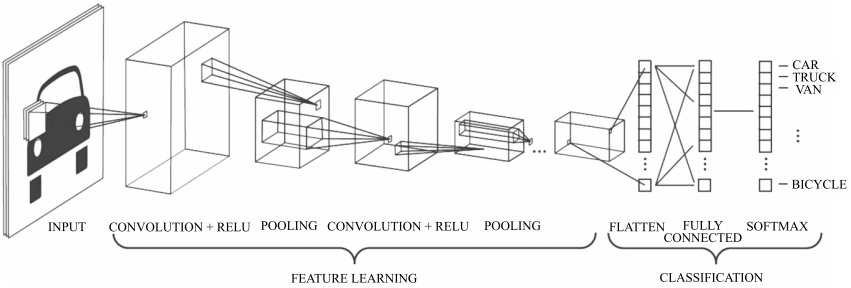


Рис. 5.5. Згорткові нейромережі

volutional Recurrent Neural Networks), генеративно-протилежні нейромережі (Generative Adversarial Networks), мережі асоціативної пам'яті (Hopfield Networks, Boltzmann Machines), мережі денної пам'яті (Memory Networks), генеративні адверсаріальні мережі (Generative Adversarial Networks, GAN) та інші [12]. Архітектури нейромереж постійно розвиваються та модифікуються з метою підвищення ефективності навчання, зменшення помилок в роботі, виконання складних комплексних завдань.

З точки зору прикладного програмного забезпечення, при реалізації функцій нейромережі, можна визначити три рівня (рис. 5.6):

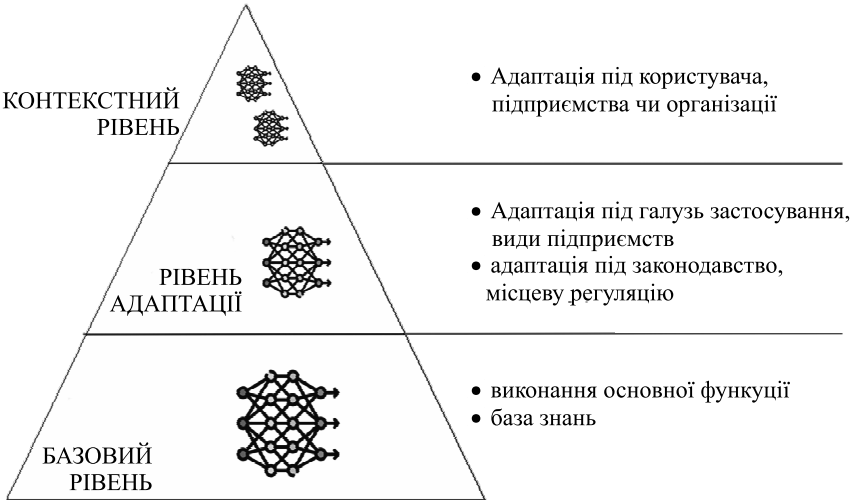


Рис. 5.6. Згорткові нейромережі

● *Базовий рівень* — це основана частина нейромережі, яка формується в процесі основного глибокого навчання;

● *Рівень адаптації* — це адаптація під певну організацію, користувача, законодавство і цей рівень містить унікальний досвід кожної практичної реалізації нейромережі;

● *Контекстний рівень* — результат навчання нейромережі при взаємодії конкретних суб'єктів з нею, тобто контекст конкретного користувача чи організації.

Отже, нейромережі є сучасним потужним інструментом ШІ, який здатний моделювати та симулювати роботу людського мозку. Цифровізація, BigData та можливість обробляти великі масиви даних забезпечили для цього необхідний ресурс.

Таким чином, теоретичними і математичними основами ШІ є кібернетика, теорія інформації, теорія обчислень за допомогою цифрових операцій,

логіка, нейропсихологічна теорія, теорія нейронних мереж, теорія навчання заснована на кон'юнктурі нейронних мереж та синапсів, математична (комп'ютерна) модель мозку. Моделі ШІ на основІ нейромереж використовуються для розв'язання складних задач, які не завжди можна вирішити за допомогою математичних формул або правил. Вони здатні до навчання на основі великих обсягів даних та розпізнавання складних залежностей у цих даних. Можуть застосовуватись в різних технологічних продуктах та галузях, зокрема у кібербезпеці та кіберрозвідці.

5.2. Основні моделі та методи штучного інтелекту

ШІ охоплює машинне навчання, планування, робототехніку, експертні системи, обробку природної мови, синтез тексту та мови, комп'ютерний зір [13—15]. Розглянемо більш детально основні моделі та методи ШІ з огляду на можливості їх застосування у кібербезпеці та кіберрозвідці.

1. *Машинне навчання (Machine Learning, ML)* — клас методів ШІ, що поєднує підходи та технології для створення алгоритмів, здатних самостійно навчатися на основі даних і знаходити приховані закономірності, що дає змогу робити прогнози на основі нових, подібних даних без необхідності явного програмування для кожного завдання. Ця технологія знаходить застосування в різних сферах, таких як розпізнавання зображень і мови, обробка природної мови, рекомендаційні системи, виявлення шахрайства, оптимізація портфелів і автоматизація завдань [16]. Існує безліч різних типів ML-алгоритмів, кожен із яких підходить для вирішення певних завдань. До найбільш поширених типів можна віднести:

1.1. *Кероване навчання* (контрольоване навчання, навчання під наглядом, або навчання з учителем) (Supervised Learning, SL) — тип машинного навчання, коли модель навчається на маркованих даних — тобто кожний вхідний приклад має відповідну правильну відповідь. Мета керованого навчання — робити точні прогнози, коли їй надають нові, невідомі дані [17]. Кероване навчання може бути застосоване до двох основних типів завдань:

Регресія — метод навчання з учителем, у якому алгоритм навчається передбачати безперервні значення на основі вхідних ознак. Різні алгоритми регресії в машинному навчанні включають: лінійну регресію (Linear Regression); поліноміальну регресію (Polynomial Regression); гребеневу регресію (Ridge Regression); регресію на основі дерева рішень (Decision Tree Regression); регресію випадкового лісу (Random Forest Regression); регресію опорних векторів (Support Vector Regression).

Класифікація — метод навчання з учителем, у якому алгоритм навчається призначати вхідні дані до певної категорії або класу на основі вхідних ознак. Алгоритми класифікації можуть бути: бінарними, коли вихід належить одному з двох можливих класів, або багатокласовими, коли вихід може належати до одного з кількох класів. Різні алгоритми класифікації в машинному навчанні включають: логістичну регресію (Logistic Regression); метод наївного Баєса (Naive Bayes); дерево рішень (Decision Tree); машину опор-

них векторів (Support Vector Machine, SVM); метод найближчих сусідів (K-Nearest Neighbors, KNN).

1.2. *Некероване навчання (Unsupervised Learning), неконтрольоване навчання, навчання без нагляду, навчання без учителя* — метод машинного навчання, що працює з немаркованими даними. На відміну від керованого навчання, де дані позначені певною категорією або результатом, алгоритми некерованого навчання спрямовані на виявлення шаблонів і взаємозв'язків у даних без попередніх знань про їх значення. Є три основні типи алгоритмів, які використовуються некерованого навчання: кластеризація, асоціативне навчання, виявлення аномалії [18].

Некероване навчання допомагає виявляти незвичайні патерни в мережевому трафіку, які можуть бути ознаками зловмисної діяльності або експлуатації невідомих вразливостей [19]. Алгоритми можуть навчатися нормальної поведінки системи та виявляти відхилення, які можуть свідчити про експлуатацію нових вразливостей.

1.3. *Зниження розмірності (Dimensionality Reduction)* — метод машинного навчання, який використовується для зменшення кількості ознак у наборі даних, зберігаючи при цьому якомога більше важливої інформації. Дозволяє зменшить складності моделі та покращити її здатності до узагальнення. Є два основних метода зменшення розмірності: вибір ознак — передбачає вибір підмножини початкових ознак, які є найбільш релевантними для вирішення задачі; видобування ознак — передбачає створення нових ознак шляхом комбінування або перетворення початкових ознак.

Методи видобування ознак: аналіз головних компонент (Principal Component Analysis, PCA); лінійний дискримінантний аналіз (Linear Discriminant Analysis, LDA); стохастичне вкладення сусідів (t-distributed Stochastic Neighbor Embedding, t-SNE).

1.4. *Напівкероване навчання* (Semi-supervised learning) — метод машинного навчання, який знаходиться між керованим та некерованим навчанням, який використовує невелику кількість маркованих даних та велику кількість немаркованих даних для навчання моделі. Мета напівкерованого навчання — навчити функцію, яка зможе точно передбачати вихідну змінну на основі вхідних змінних, подібно до керованого навчання.

Типи напівкерованого навчання: самонавчання (Self-training, Self-labeling); спільне навчання (Co-training); генеративні моделі (Generative Models); методи на основі графів (Graph-based Methods); регуляризація узгодженості (Consis tency Regularization); розділення низької щільності (Low-density Separation).

1.5. *Навчання з підкріпленням (Reinforcement learning, RL)* — метод машинного навчання, зосереджений на прийнятті рішень з метою максимізації накопиченої винагороди в заданій ситуації. На відміну від керованого навчання, яке ґрунтується на тренувальному наборі даних із заздалегідь визначеними відповідями, навчання з підкріпленням передбачає навчання через досвід. У навчанні з підкріпленням агент навчається досягати цілі в неви-

значеному, потенційно складному середовищі, виконуючи дії та отримуючи зворотний зв'язок у вигляді винагород або штрафів.

Навчання з підкріпленням включає різноманітні методи та алгоритми для вирішення задач прийняття рішень, де агент навчається через взаємодію із середовищем. Ці технології є основою для сучасних методів RL: динамічне програмування (Dynamic Programming, DP); методи Монте-Карло (Monte Carlo, MC); навчання з тимчасовою різницею (Temporal Difference, TD); методи на основі політики (Policy-Based Methods); методи на основі значень (Value-Based Methods); модельно-орієнтоване навчання з підкріпленням (Model-Based RL); моделезалежне навчання з підкріпленням (Model-Free RL); глибоке навчання з підкріпленням (Deep Reinforcement Learning); стратегії дослідження та експлуатації у навчанні з підкріпленням (Exploration and Exploitation Strategies); рівняння Беллмана (Bellman Equations).

1.6. *Глибоке навчання* (deep learning) — метод машинного навчання, який використовує багатошарові нейронні мережі (глибокі нейронні мережі), щоб імітувати складні можливості прийняття рішень людського мозку. Використання багатошарових нейронних мереж дає можливість автоматичного виділення характеристик і розпізнавання складних патернів у великих обсягах даних.

Глибоке навчання може бути реалізоване на основі наступних нейронних мереж: глибокі мережі з прямим поширенням (Deep Feedforward Networks, DFFN); згорткові нейронні мережі (Convolutional Neural Networks, CNNs або ConvNets); рекурентні нейронні мережі (Recurrent Neural Networks, RNNs); сіамські нейронні мережі (Siamese Networks); генеративні змагальні мережі (Generative Adversarial Networks, GANs): графові нейронні мережі (Graph Neural Networks, GNNs; моделі "трансформери" (Transformers); моделі дифузії (Diffusion Models).

2. *Планування* — різновид ШІ, який дає можливість вирішувати завдання пошуку процедурного курсу дій для систем, що описані декларативно, з метою досягнення їх цілей при оптимізації загальних показників ефективності. Автоматизовані планувальники знаходять трансформації, які потрібно застосувати в кожному даному стані серед можливих трансформацій для цього стану. На відміну від задачі класифікації, планувальники надають гарантії щодо якості розв'язку. Дають можливість створення серії дій для досягнення конкретної мети з оптимізацією ресурсів та ефективності в умовах обмежень і змінних ситуацій.

Існує кілька методів планування в ШІ, кожен з яких підходить для різних завдань та середовищ: детерміноване планування (Deterministic Planning); невизначене планування (Non-deterministic Planning); планування з обмеженнями (Consttraint-based Planning); ітераційне планування (Iterative Planning); планування для багатьох агентів (Multi-agent Planning); планування в реальному часі (Real-time Planning).

3. *Робототехніка* — важлива підгалузь ШІ, яка зосереджена на проєктуванні та створенні роботів (машин, здатних виконувати завдання автономно або напівавтоматично). Інтеграція ШІ в робототехніку покращує

здатність роботів обробляти інформацію, приймати рішення та адаптуватися до змінюваних умов. Основні напрямки роботехніки: автоматизація процесів (Robotic process automation, RPA), фізичні інтерфейси (Robotic physical interfaces, RPI).

4. *Експертні системи* — різновид ШІ, який імітує здатність до прийняття рішень людини-експерта. Ці системи використовують базу знань, заповнену специфічною для галузі інформацією та правилами, щоб інтерпретувати та вирішувати складні проблеми. Експертні системи широко використовуються в таких сферах, як медична діагностика, бухгалтерія, програмування та навіть у іграх. Основні типи експертних систем у ШІ: правило-базовані експертні системи (Rule-based Expert Systems); фрейм-базовані експертні системи (Frame-based Expert Systems); системи нечіткої логіки (Fuzzy Logic Systems); експертні системи на основі нейронних мереж (Neural Network-based Expert Systems).

5. *Обробка природної мови* (Natural Language Processing, NLP) — підгалузь ШІ, метою якої є зробити комп'ютери здатними розуміти людську мову. NLP використовує обчислювальну лінгвістику, яка вивчає, як працює мова, а також різні моделі, засновані на статистиці, машинному навчанні та глибокому навчанні. Ці технології дозволяють комп'ютерам аналізувати та обробляти текстові чи голосові дані, а також розуміти їх повне значення, включаючи наміри та емоції мовця чи автора. Обробка природної мови охоплює кілька ключових напрямів: розуміння природної мови (Natural Language Understanding, NLU); генерація природної мови (Natural Language Generation, NLG); машинний переклад (Machine Translation); розпізнавання мови (Speech Recognition); синтез мови (Speech Synthesis); аналіз настроїв (Sentiment Analysis); витягування інформації (Information Extraction); діалогові системи (Dialogue Systems);

Ці підгалузі взаємодіють між собою, сприяючи розвитку технологій, що дозволяють комп'ютерам ефективно взаємодіяти з людською мовою.

6. *Комп'ютерне мовлення* — підгалузь ШІ яка зосереджена на обробці, розумінні та генеруванні людської мови в усній формі, що дає можливість машинам взаємодіяти з людьми за допомогою голосу. Охоплює таки основні напрямки, як: перетворення мовлення в текст (Speech-to-text), перетворення тексту в мовлення (Text-to-speech).

7. *Комп'ютерний зір* (Computer vision) — підгалузь ШІ, яка зосереджена на тому, щоб дозволити комп'ютерам аналізувати та отримувати інформацію із зображень і відео, подібно до людського зору. Вона передбачає розробку алгоритмів та методів для отримання значущої інформації з візуальних даних і розуміння навколишнього візуального світу. Основні напрямки є розпізнавання зображень (Image Recognition) і машинний зір (Machine vision).

Отже, проведений аналіз основних моделей і методів ШІ свідчить про достатньо широкі можливості застосування ШІ в різних галузях, зокрема в оборонних інноваціях, що може призвести до підвищення ефективності їх заходів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лисецький Ю. М., Сокур В. В. Теоретичні та математичні основи штучного інтелекту. *Вісник воєнної розвідки*. 2024. № 85. С. 51–56.
2. Norbert Wiener. Cybernetics or Control and Communication in the Animal and the Machine, Paris — Cambridge, Mass. 1948. 194 p.
3. Shannon C. E.. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948. T. 27. C. 379–423.
4. A. M. Turing. Computing Machinery and Intelligence. Mind № 49. 1950. C. 433–460.
5. Warren S. McCulloch and Walter Pitts, A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*. Vol. 5. 1943.pp. 115—133 .
6. Donald Olding Hebb The Organization of Behavior: A Neuropsychological Theory. D.O. Hebb: The Organization of Behavior, Wiley: New York; 1949. 337c.
7. Кононюк А.Ю. Нейроні мережі і генетичні алгоритми — К.: «Корнійчук». 2008. 446 с.
8. Rosenblatt, Frank. The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain, Cornell Aeronautical Laboratory, Psychological Review, v65, No. 6, 1958. pp. 386—408.
9. Калбазов Д.Й., Данченко О.І., Лисецький Ю.М. Нейромережі. Розвиток та перспективи. *Математичні машини і системи*. 2024. № 2. С. 24—32.
10. What is Perceptron? A Beginners Guide for 2023. URL: https://www.simplilearn.com/tutorials/deep-learning-tutorial/perceptron (дата звернення 15.09.2024).
11. 7 архитектур нейронных сетей для решения задач NLP. URL: https://neurohive.io/ru/osnovy-data-science/7-arhitektur-nejronnyh-setej-nlp/ (дата звернення 23.09.2024).
12. Які існують типи нейронних мереж? URL: https://devzone.org.ua/qna/iaki-isnuiut-tipi-neironnix-merez (дата звернення 23.09.2024).
13. Artificial Intelligence. URL: https://www.britannica.com/technology/ artificial-intelligence (дата звернення: 22.11.2024).
14. Ravil Mukhamediev, Yelena Popova, Yan Kuchin, Elena Zaitseva. Review of Artificial Intelligence and Machine Learning Technologies: Classification, Restrictions, Opportunities and Challenges. Mathematics. 2022. URL: https://www.mdpi.com/2227-7390/10/15/2552 (дата звернення: 22.11.2024).
15. Сокур В.В., Лисецький Ю.М. Аналіз можливостей застосування штучного інтелекту у пентесті та етичному хакінгу. *Вісник воєнної розвідки*. 2025. № 86. С. 53—58.
16. K. Jeevan Kumar, K. Jairam, & Ch.Ambedkar.. An In-Depth Study Of Machine Learning In Artificial Intelligence. 2023. *Educational Administration: Theory and Practice*, *29*(4), 2401—2408. URL: https://doi.org/10.53555/kuey.v29i4.7127 (дата звернення: 22.11.2024).
17. Supervised learning URL: https://itwiki.dev/data-science/ml-reference/ml-glossary/supervised-learning (дата звернення: 22.11.2024).
18. D. Peer. Implementing real-time anomaly detection in network traffic using machine learning. 23.09.2024. URL: https://peerdh.com/uk/ blogs/programming-insights/implementing-real-time-anomaly-detection-in-network-traffic-using-machine-learning (дата звернення: 22.11.2024).
19. Yevhen Chychkarov, Olga Zinchenko, Andriy Bondarchuk, Liudmyla Aseeva. Detection of network intrusion using machine learning and fuzzy logic. 2023. *Cybersecurity: Education, Science, Technique*. 1. P. 234-251.

РОЗДІЛ 6
ДЕЗІНФОРМАЦІЯ В КОНТЕКСТІ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ ТА КОГНІТИВНИХ ВОЄН СУЧАСНОСТІ

Дар'я ДЗЯДУК,
доктор філософії, старший дослідник

Сучасні міждержавні конфлікти із сукупністю застосовуваних конвенційних та неконвенційних методів ведення боротьби піднімають на гора проблему виникнення нового балансу сил, що призводить до утворення нового світового порядку. Процеси активної трансформації інформаційного поля, переорієнтація, деформація та переформатування традиційних медіаканалів розповсюдження інформації, а також стрімка їх диджиталізація сприяли активному розгортанню когнітивних та консцієнтальних війн суб'єктів глобальних геополітичних протистоянь в рамках гібридної війни як комплексного формату батальної взаємодії сторін, а також боротьби за сірі зони стратегічної конкуренції.

Ще свого часу філософ та дослідник впливу медіа як засобу комунікації на аудиторію Маршал Маклюен (1911—1980) зауважував, що інформація відіграватиме головну роль у війнах майбутнього. На його думку, медіа сприяють формуванню образів ворога в масовій свідомості, і в цілому характеризував сучасну йому епоху, як епоху війни інформації, в якій медіа виявляється зброєю сильнішою за традиційну. З огляду на роль інформації в сучасному світі М. Маклюен стверджував, що істинно тотальна війна — це війна за допомогою інформації [1]. У цьому розумінні гібридна війна є не тільки війною, що використовує інформацію як зброю, а й війною цінностей, війною за громадську думку, емоції та свідомість.

Концепція когнітивної війни виникла на перетині військових, інформаційних та психологічних досліджень. Її коріння можна знайти в різних військових доктринах і стратегічних підходах до інформаційної та психологічної війни, але як окремий термін вона набула широкого використання в останні десятиліття. Один із перших офіційних військових документів, що прямо посилається на когнітивну війну, з'явився в НАТО, зокрема в рамках діяльності Allied Command Transformation (ACT), яке активно досліджує нові загрози, зокрема пов'язані з інформаційними та когнітивними впливами [2]. Командування трансформації союзників (Allied Command Transformation) керує концепцією дослідження когнітивної війни, яка є частиною ширшого порядку денного розвитку військових стратегій. Розуміння концептуальних рамок, визначень, наслідків і ризиків такої війни, на думку спеціалістів, сприяє кращому ухваленню політичних рішень, розвитку військових спроможностей і забезпеченню загальної безпеки Альянсу. Командування трансформації союзників здійснює навчання, співпрацю, захист та формування

спроможностей НАТО у сфері когнітивної війни, надаючи рекомендації щодо підвищення обізнаності, цивільно-військової співпраці, стійкості суспільства та обміну даними для забезпечення нинішньої та майбутньої безпеки Альянсу.

Спрямована на зміну сприйняття реальності, загальносуспільна маніпуляція стала новою нормою, а людська когніція перетворюється на критичну сферу ведення війни. Визначення когнітивної війни, запропоноване у дослідницькій концепції НАТО ACT, є таким: "Діяльність, що проводиться у синхронізації з іншими інструментами влади з метою впливу на ставлення та поведінку шляхом маніпулювання, захисту або порушення когніції окремих осіб і груп для отримання переваги над противником" [3].

Актуальність цієї концепції випливає з викликів, з якими НАТО зіштовхнулося останніми роками і внесло до концепції, а саме [3]:

• технологічний прогрес і зміни у споживанні інформації надають противникам більші можливості для збору та маніпулювання даними, впливу на емоції, формування переконань і поведінки. Це дає можливість використовувати розбіжності в суспільстві через новітні технології, такі як штучний інтелект, передові та проривні технології (EDTs), збір даних. Крім того, поширення соціальних медіа сприяє впливу на думки, емоції та дії окремих осіб.

Як зазначають автори концепції, це є відображенням тактики гібридної війни, де суспільство використовується як вектор впливу на ключові цілі — політичних і військових лідерів. Ефективність інформаційних кампаній залежить від цілеспрямованої маніпуляції емоціями та когнітивними схильностями, що спричиняє масштабні зміни у ставленнях і поведінці. Такі зміни часто є тонкими й малопомітними, стираючи межу між справжніми суспільними дискусіями та ворожими когнітивними атаками, які експлуатують соціальні розбіжності;

• Хоча когнітивні атаки не є новим явищем, концепція визначає їх як навмисні наступальні маневри, спрямовані на вплив на сприйняття, переконання, інтереси, рішення та поведінку через пряму атаку людської свідомості. Інноваційність підходу полягає в тому, що противники тепер можуть швидко та анонімно здійснювати когнітивні атаки в інформаційному середовищі, використовуючи цифрові платформи та проривні технології ШІ.

Когнітивні війни сучасності цілком відображають систему принципів філософської епохи метамодерну, для якої такі категорії, як істина чи правда є абсолютно відносними. Якщо постмодернізм був позначений зростанням впливу ЗМІ на формування нових принципів сприйняття дійсності індивідом, нового типу міждержавної комунікації, а телебачення сприяло культивуванню масової попкультури, то початок XXI століття породив нове явище, а саме Інтернет, який трансформував взаємини по горизонталі "суб'єкт—об'єкт", у випадку духовно-інформаційного обміну — "автор–реципієнт". Наприклад, голосування за учасників різнорідних ТБ-шоу стає недостатнім актом комунікації для людини нової інформаційної доби, оскільки вона має на меті бути не тільки на стороні об'єкта чи суб'єкта цієї комунікації, а

втілювати одночасно дві ці ролі. Цю докорінну зміну функції продуцента відмічає А. Кірбі: “автор відтепер має статус одного з тих, хто задає параметри, без яких інші оператори стають просто не релевантними, невідомими, поза лінією. Ці ж зміни стосуються і власне самого “тексту”, що характеризується тепер гіперефемерністю і нестабільністю” [4].

Сьогодні великої популярності в Європі набуває проєкт Metamoderna.org [5] — колаборація шведських культурологів і соціологів Еміля Фріїс та Даніеля Гьорца, задля створення віртуального “філософа, історика і соціолога” Ханзі Фрайнахта, який “живе” на самоті в швейцарських Альпах. Поєднавши вікову психологію та культурологічні дослідження, Еміль Фріїс і Даніель Гьорц від імені Ханзі Фрайнахта нещодавно видали книгу “The Listening Society”, де розкрили таємниці “мему метамодерного значення” [6]. Людина цієї доби перебуває серед надлишку інформації, фактів, подій, знань, речей, у цей час складно і вже не потрібно прагнути до стабільності або кінцевої системи як істинності. Світ постправди, фейкових новин та інформаційних маніпуляцій відводить від відчуття стабільності та розуміння суті дійсності.

Метамодерн породив нову хвилю інформатизації суспільства з утвердженням мережі Інтернет, а згодом і штучного інтелекту, розширенням доступу до цих технологій представників суспільства з різним достатком, а також формуванням так званих нових медіа в соціальних мережах (блогів, пабліків, публічних сторінок тощо). Саме інтернет-комунікація призвела до трансформації міжособистісного, міжінституціонального та міждержавного інформаційного обміну. У цей час завдяки глобальній онлайн-павутині виникають та утверджуються такі поняття, які активно використовуються в рамках когнітивних воєн:

“post-truth” — “постправда” виникла як феномен доби постмодерну, але у метамодерні довершується та стає маркером інформаційного часу. Відповідно до “Оксфордського словника англійської мови” постправда — інформаційний потік, який навмисно конструюється в сучасному суспільстві за допомогою ЗМІ для створення віртуальної, відмінної від дійсності, реальності з метою маніпулювання суспільною свідомістю [7]. У 2016 році це слово редакторами словника було названо словом року;

“cancel culture” — “культура скасування” — сучасна форма остракізму, яку професор Університету штату Мічиган Ліза Накамура назвала прагненням контролювати свободу думок, користуючись владою, яку дали соціальні мережі [8]. Йдеться про цькування публічних особистостей в інформаційному просторі за вчинки та дії в теперішньому чи минулому, в умовах загального права на самовираження та висловлення власної позиції в мережі. Таким чином перестає працювати презумпція невинуватості на рівні суспільних обговорень. Такі інформаційні мережеві кампанії також іноді називають “канселлінг”;

“deepfake” — буквально — глибинна підробка. Методика синтезу зображення людини, яка ґрунтується на штучному інтелекті. Вона викори-

стовується для поєднання і накладання зображень та відео на початкові зображення або відеоролики. Методи виявлення жестів та перетворення початкового відео на відео з особою, схожою на цільову особу, були представлені в 2016 році і дають можливість обчислення в режимі реального часу підроблених мімічних виразів в 2D-відео [9]. Дипфейки можуть бути використані для створення підроблених новин, зловмисних обманів, зокрема компрометації знаменитостей, публічних осіб та знищення політичної репутації;

“metaverse” (метавсесвіт) — термін, який винник у науково-фантастичних романах у 1990-х. Восени 2021 року Марк Цукерберг актуалізував його, представивши курс концептуального ребрендингу компанії “Facebook”, яка тепер працюватиме над створенням нової кіберреальності, в якій симулякри стають інструментом докладного відтворення реальності в кіберпросторі. За задумом метавсесвіт — це постійний живий віртуальний простір, у якому люди можуть взаємодіяти один з одним і з цифровими об’єктами через свої аватари, за допомогою технологій віртуальної реальності [10].

Метамодерна свідомість перебуває в процесі постійної осциляції (розгойдування). Йдеться про радикальну відкритість, про всеприйняття. У цей час когнітивні війни набувають свого розквіту, оскільки Інтернет, ШІ та соціальні мережі як головний маркер нових інформаційно-духовних обмінів став причиною появи метамодерного автора та метамодерного реципієнта, які часто міняються ролями (це можна представити у вигляді посту з певною інформацією у соціальних мережах, який тиражують інші користувачі на своїх сторінках, оздоблюючи його безліччю коментарів та супровідних текстів). Людська свідомість починає постійно перебувати у стані “мета” — “між” звичною реальністю, та мережевою реальністю, яка максимально дублює об’єктивну дійсність; між правдою та неправдою, довірою та недовірою.

З огляду на стрімке утворення нової інформаційної реальності, що ґрунтується на кібертехнологіях, зокрема й ШІ, можна припустити, що людство перебуває на етапі формування нового типу суспільства метамодерну — інформаційно-мережевого, яке перманентно перебуває в стані когнітивної та консцієнтальної війни. Маніпуляція свідомістю за допомогою інформації поступово замінила собою насильство, що тривалий час вважалося єдиним засобом правління. Саме тому сучасні медіа такого типу стають ефективним інструментом політичної пропаганди, поширення дезінформації джерелом дестабілізаційних соціальних процесів, а також безпосередньо інформаційною зброєю, яка використовується в рамках гібридних воєн. Під час такої когнітивної війни активно використовують сучасні кібертехнології, зокрема штучний інтелект.

Захист віртуального простору від поширення когнітивних атак — новий етап розвитку інформаційної безпеки, який спрямований саме на диджитал середовище. У кінці 90-х експерти аналітичного центру RAND адміністрації США Дж. Аркілла і Д. Ронфельд висвітлили проблеми ін-

формаційної стратегії, кібервійни, мережевої війни та інформаційної війни. На їхню думку, слід було об'єднати поняття кіберпростору та інформаційної сфери як сукупності кіберпростору і засобів масової інформації в єдину "ноосферу" — нову, засновану на ідеях, духовних цінностях, етиці, епістемологічній парадигмі, в якій на зміну традиційній політиці "грубої" сили з її акцентом на матеріальну складову протиборства приходить нова, заснована на "м'якій силі". Сучасній "ноовійні" як війні смислів, знань відповідає і спеціальний термін для нової політики — "ноополітіка" [11]. Така політика здійснюється як у реальному так і віртуальному просторі, відповідно використовує різні майданчики для своєї реалізації, а також різні інструменти.

Дезінформація, підтримувана іноземними державами, може мати на меті створення плутанини, загострення політичної поляризації, підрив демократії або формування недовіри в суспільствах. Хоча дослідження свідчать про те, що дезінформація може впливати на переконання, ступінь, до якого вона призводить до змін у поведінці або має реальний вплив, залишається невизначеним і складним для вимірювання. У січні 2024 року Всесвітній економічний форум назвав дезінформацію найбільшим короткостроковим ризиком у світі через її потенційну загрозу підриву демократичних виборів, спричинення суспільних заворушень і посилення цензури через ініціативи протидії дезінформації [12].

Цифровий простір стає специфічним майданчиком для інформаційного тероризму, когнітивних та консцієнтальних атак, симульованих війн, війн Гібсона. Якщо перша категорія є найрозповсюдженішим видом інформаційної агресії в цифровому просторі, то когнітивні атаки полягають у збереженні роботи інформаційної системи в коректному вигляді, але з певним викривленням, зміною інформаційного потоку, який змінює принцип сприйняття інформації, а згодом і здатності до коректного її аналізу, в залякуванні певним видом зброї з відповідним інформаційним супроводженням, що має особливі технічні характеристики. Війни Гібсона існують скоріше як концепт, який полягає у веденні війни у віртуальному просторі за допомогою інтелекту (включення людини безпосередньо в мережу Інтернет) [13]. Таким чином технології штучного інтелекту інтегровані у так звану неополітику.

Варто зауважити, що штучний інтелект у сфері когнітивної війни може суттєво розширити масштаби загрози масової зміни свідомості. Як відомо, одним із трьох стовпів функціонуючої демократії є представництво. Для того щоб обрані представники ефективно відповідали на запити своїх виборців, вони мають точно знати, що ті думають. Проте інформаційна війна, керована ШІ, може маніпулювати соціальними мережами, створюючи плутанину та поширюючи дезінформацію, що спотворює сприйняття політиками суспільних настроїв. Таким чином, якщо населення демократичних країн буде введене в оману і повірить, що, наприклад, Україна та Тайвань не варті захисту, світ стане критично вразливими до агресивної тиранії.

У рамках Мюнхенської конференції з безпеки 2024 року було прийнято документ “Битва за розум: розуміння та подолання когнітивної війни і її новітніх технологій” [14], який узагальнює дискусії, що відбулися під час круглого столу високого рівня з питань когнітивної війни, організованого Центром з питань управління змінами (CGC) Університету IE. У заході взяли участь Маргрете Вестагер, Аранча Гонсалес Лайя, Енн-Марі Слотер та інші відомі політики й лідери галузі. У документі аналізується становлення когнітивного простору як шостого виміру війни — після суші, моря, повітря, космосу та кіберпростору, в контексті мультидоменної теорії.

Сьогодні як державні, так і недержавні актори мають засоби та стимули для маніпулювання нашими думками та руйнування спільного уявлення про реальність — від перешкоджання конкретним військовим маневрам до дестабілізації суспільств і багатостороннього співробітництва. Сучасне суспільство увійшло в гіперреалістичний сон, в якому все є правдою і неправдою одночасно, і той, хто генерує смисли та інформацію, сам потрапляє в її лабети, стаючи вже споживачем, а не продуцентом. Збільшення активності використання штучного інтелекту в усіх галузях діяльності люди не тільки конструктивно впливає на розвиток високих технологій, поліпшує можливості забезпечення індивідуальної та національної безпеки, але і стає інструментом дестабілізаційних процесів, як в середині мікрокосму окремо взятої особистості, впливаючи на процеси обробки нею інформації, але і в геополітичному макрокосмі, навіть трансформуючи розуміння усталеного світопорядку. Зростання використання оманливих наративів і маніпулятивного ШІ в демократичних процесах, війна в Україні та конфлікт між Ізраїлем і ХАМАС свідчать про зростаючий геополітичний інтерес до контролю над сприйняттям людей. Громадяни ліберальних демократій особливо вразливі до когнітивних маніпуляцій, оскільки економія уваги негативно впливає на нашу здатність до критичного мислення, довіра до інституцій перебуває на безпрецедентно низькому рівні, а поляризація суспільства досягла свого піку.

Наприклад, Народно-визвольна армія Китаю (НВАК) активно розвиває те, що вона називає когнітивною війною. Її мета — маніпулювати розумовими процесами противника різними способами для досягнення бажаних результатів. Філософія конфлікту Комуністичної партії Китаю (КПК) еволюціонує до сприйняття людського мозку як окремого операційного простору. Китайське бачення передбачає створення інтегрованої системи систем, у якій люди будуть взаємодіяти з інформаційними технологіями (ІТ) та отримуватимуть когнітивні посилення в межах певного типу трансгуманістичної еволюції [15]. У цій концепції перемоги війна більше не передбачає знищення ворожих військових формувань на полі бою. Натомість формується новий підхід до ведення бойових дій, у якому одна система здатна поглинути, порушити, паралізувати або повністю знищити здатність ворожих систем функціонувати, не кажучи вже про ведення традиційного військового наступу.

Останніми роками спостерігається значне зростання використання штучного інтелекту для створення дезінформації та пропаганди. Зокрема, з кінця 2023 року, коли генератори зображень на основі ШІ стали широко доступними, частка фейкових зображень, створених за їх допомогою, істотно зросла. До початку 2023 року такі зображення становили незначну частку маніпуляцій, але згодом їхня кількість почала швидко збільшуватися. Дослідження Arxiv 2023 року показало, що кількість синтетичних новин зросла на 57,3% на традиційних сайтах та на 474% на дезінформаційних ресурсах протягом 2022—2023 років [16].

Згенерований контент виглядає дуже реалістично, деякі зі стратегій, які наразі використовуються для виявлення маніпулятивних акаунтів і контенту, стають неефективними під час виявлення чи запобігання дезінформації, створеної штучним інтелектом. Чим дезінформація, згенерована штучним інтелектом, відрізняється від традиційної, створеної людиною? Штучний інтелект може неабияк посилювати проблему поширення та створення дезінформації через кілька ключових аспектів:

масштаб і швидкість поширення — ШІ штучний інтелект дає можливість масово створювати контент для дезінформаційних кампаній, що може призводити до збільшення кількості фейкових історій, різних варіацій одного й того ж сюжету, генерація його різними мовами, автоматизованих діалогів тощо. Порівняно з ручним створенням контенту, технології ШІ дозволяють продукувати дезінформацію за лічені секунди. Ці два фактори — масштаб і швидкість — становлять серйозний виклик для фактчекерів, які будуть змушені працювати в умовах постійного потоку дезінформації. Медіапростір, можна припустити, у недалекому майбутньому буде захлинатися в масиві такої інформації, оскільки перевірка фактів потребуватиме чимало часу;

доступність — активне поширення інструментів ШІ ліквідує бар'єри для проведення інформаційних операцій. Люди різного достатку, статусу та соціального становища зможуть створювати реалістичні фейкові зображення та відео без професійних навичок чи складного редагування. Це може призвести до "демократизації" фабрик тролів;

переконливість контенту — глибокі нейромережі можуть генерувати правдоподібні тексти, фото та відео (наприклад дипфейки), які складно відрізнити від реальних. Необхідно зважати на те, що у часи кліпового мислення сприйняття інформації відбувається фрагментарно, швидко та поверхнево, а сенсаційна візуалізація інформації інструментами ШІ, якщо може і не сприйнятися як беззаперечна правда, але беззаперечно лишить певний психологічний якір, який надалі буде впливати на сприйняття та аналіз наступної інформації з цієї ж теми;

таргетинг і персоналізація — технології ШІ дають можливість запускати персоналізовані кампанії з дезінформації, орієнтовані на конкретні аудиторії (або навіть окремих осіб) з урахуванням їхніх уподобань чи переконань, навіть без глибокого знання мови чи культури цільової групи. ШІ здатний експериментувати в реальному часі, спостерігаючи за поведінкою

людей та швидко визначаючи найбільш ефективні стратегії й тактики. Це дає змогу йому вдосконалюватися набагато швидше, ніж людині. Наприклад, така дезінформація може бути спрямована на людей різного віку, політичних поглядів, релігійних переконань або особистісних психотипів (наприклад, екстравертів чи інтровертів), що підвищує її ефективність. Особливо вразливими можуть бути люди, які вже зазнають соціальної маргіналізації або мають низьку медіаграмотність. Крім того, ШІ може аналізувати цифрову активність і фінансові транзакції, створюючи психологічний профіль або цільовий пакет даних майже для кожної людини;

автоматизація маніпуляцій — боти та алгоритми можуть імітувати людську активність у соцмережах, створюючи ілюзію підтримки певних ідей або тиску на громадську думку. Крім того, це дає можливість суттєво зменшити фінансові витрати на такі інформаційні кампанії, зокрема завдяки скороченню кількості залучених спеціалістів для їх реалізації;

підрив довіри до правди — велика кількість якісного фейкового контенту може спричинити загальну недовіру до всіх джерел інформації, ускладнюючи пошук правди і викликати ефект ерозії правди.

Теоретично, якщо ШІ визначить, що ціль має нейротичні риси, він зможе створити пропагандистське повідомлення, яке викликатиме сильний стрес, до якого така особа більш вразлива. Попри те, що штучний інтелект ще не здатен діагностувати розлади, він швидко розвивається у цьому напрямі. Наприклад, якщо солдата буде ідентифіковано як депресивного, ШІ потенційно може спробувати спровокувати самогубство.

Як всі ці риси ШІ можуть втілюватись у реальні кейси на прикладі війни в Україні? Неодноразово було застосовано таку тактику: ШІ збирав фотографії загиблих солдатів, порівнював обличчя з фото у соцмережах, ідентифікував їх і надсилав знімки родинам загиблих. Звісно, можна просто використати дипфейк. Такі дії матимуть руйнівний психологічний ефект на родину, що, у свою чергу, підриває моральний дух і сіє страх. Ця стратегія також може перевантажити командування тилових підрозділів та психологічні служби гарнізону. Якщо ж солдати на передовій дізнаються про подібні випадки, це може мати серйозний деморалізуючий вплив.

Масове створення контенту може посилити тактики, спрямовані на відволікання аудиторії та створення ілюзії більшості (оскільки контент виглядає так, ніби надходить із різних джерел). Наприклад, державні та пов'язані з державою актори, такі як російське "Агентство інтернет-досліджень", уже давно використовують сотні акаунтів для відволікання уваги від незручних тем, і з появою генеративного ШІ ця практика стає ще простішою. У той же час створення автоматизованих діалогів у реальному часі може допомогти замаскувати ботів та зробити їхні акаунти в соціальних мережах більш правдоподібними.

Щороку кількість загальнодоступних програм ШІ невпинно збільшується, й щоразу кожна з них стає свідченням не тільки активного розвитку кібертехнологій, але і джерелом небезпеки для інформаційно-комунікацій-

ної сфери й національної безпеки загалом. З огляду на різноманіття програм зі штучним інтелектом типологічно їх можна поділити за такими критеріями: за рівнем розвиненості, за методами навчання, за принципом роботи, за функціональністю (табл. 1).

Таблиця 6.1. **Типи програм на основі ШІ за різними критеріями**

ТИП ПРОГРАМИ	ОПИС АЛГОРИТМУ
За рівнем розвиненості	
Низький рівень (ANI, Narrow AI)	спеціалізований ШІ, який виконує одну конкретну задачу (наприклад, голосові асистенти, пошукові алгоритми, системи рекомендацій)
Середній рівень (AGI, General AI)	гіпотетичний ШІ, здатний мислити та навчатися, як людина, адаптуючись до нових завдань
Високий рівень (ASI, Super AI)	поки що теоретичний рівень, на якому ШІ перевершує людський інтелект у всіх сферах
За методами навчання	
Машинне навчання (Machine Learning)	ШІ навчається на основі даних і статистичних методів
Глибоке навчання (Deep Learning)	використовує нейронні мережі для аналізу складних патернів
Еволюційні алгоритми	імітують процес природного відбору для пошуку оптимальних рішень
За принципом роботи	
Символьний ШІ (Symbolic AI)	працює на основі логічних правил і знань
Нейромережевий ШІ (Neural Networks AI)	використовує штучні нейронні мережі, натхненні людським мозком
Гібридний ШІ	поєднує кілька підходів для підвищення ефективності
За функціональністю	
Реактивний ШІ (Reactive AI)	реагує на вхідні дані, не має пам'яті (наприклад, шаховий комп'ютер Deep Blue)
ШІ з обмеженою пам'яттю (Limited Memory AI)	враховує попередні дані (наприклад, автопілоти в авто)
Теоретично мислячий ШІ (Theory of Mind AI)	гіпотетична система, яка розуміє емоції та наміри людей
Самоусвідомлений ШІ (Self-aware AI)	перебуває в теорії, прогнозується створення ШІ з власною свідомістю

Та, для розуміння інструментарію ШІ-дезінформації розгляньмо кілька програм, які найчастіше використовуються для генерації та поширення неправдивої інформації.

GPT-3 та GPT-4 (OpenAI)

Ці мовні моделі можуть генерувати реалістичний текст, який використовується для створення фейкових новин, статей, а також для автоматизації коментарів і повідомлень у соцмережах. Вони можуть імітувати стиль відомих джерел, що робить їх ідеальними для створення дезінформації.

DeepAI та інші програми для створення дипфейків

Генерація фальшивих відео за допомогою алгоритмів дипфейк є однією з найефективніших і найшкідливіших форм дезінформації. Інструменти на кшталт DeepAI, FakeApp, 4Reface або Deep FaceLab дають можливість створювати реалістичні відео за заданими параметрами з будь-якою особовою в головній ролі, прописуючи сценарії її дій таким чином, що це стає надзвичайно переконливим для таргет аудиторії.

Artbreeder

Це інструмент на базі штучного інтелекту, що дає можливість створювати реалістичні зображення на основі генетичних алгоритмів. Його використовують для створення фальшивих профілів людей або маніпуляцій із зображеннями для дезінформаційних кампаній.

Synthesia

Програма для створення відео з аватарами, що використовуються для синтезу фальшивих новин або заяв від імені публічних осіб.

Lyrebird (Descript)

Ця платформа дає можливість створювати аудіо-файли, що точно імітують голоси людей, використовуючи штучний інтелект. Вона активно використовується для створення фальшивих записів, якфі можуть бути використання для маніпулювання громадською думкою або у дискредитаційних кампаніях.

BERT (Bidirectional Encoder Representations from Transformers)

Моделі на основі BERT активно використовуються для аналізу тексту, створення фальшивих коментарів або відгуків у соцмережах, а також для виявлення націлених маніпуляцій.

ChatGPT

Цей чат-бот може бути використаний для автоматизованих бесід, поширення пропаганди, а також для маніпулювання дискусіями, створення підроблених текстових діалогів, що виглядають правдоподібно.

TuringBot

Цей бот використовує штучний інтелект для генерації текстів, які мають форму та зміст реальних новин або повідомлень. Він здатний масово виробляти фальшиву інформацію, що поширюється в інтернеті.

Grok 3

Новітня модель штучного інтелекту, розроблена компанією xAI під керівництвом Ілона Маска. Вона поєднує здатність до міркувань із великим

обсягом знань, що робить її однією з найпотужніших ШІ-систем сьогодні. Цей ШІ неодноразово опинявся в центрі уваги в наслідок своєї участі у поширенні дезінформації. Наприклад, у квітні 2024 року чатбот Grok згенерував фейкову новину про нібито атаку Ірану на Ізраїль. Ця неправдива інформація була опублікована до реальної події та згодом з'явилася в офіційному розділі популярних новин на платформі X, що збільшило її охоплення серед користувачів [17].

За допомогою описаних вище та інших програм здійснюється рефлексивне управління особистістю в рамках когнітивної війни, коли відбувається вплив на емоції, поведінку, та свідомість противника за допомогою спеціально підготовленої інформації підсиленої інструментами ШІ, яка спонукає його до прийняття бажаного рішення. Довготривалий вплив інформації, створеної ШІ впливає на когнітивні здібності особистості, а саме пригнічує їх, знищує критичне мислення та можливості до творчої самореалізації та прийняття нестандартних рішень. Це довело дослідження Microsoft та Університету Карнегі-Меллона [18], в якому взяли участь 319 IT-фахівців. Було виявлено пряму залежність між впевненістю в ШІ та зниженням критичного мислення. Критичне мислення було визначено як таке, що підпадає під одну з шести категорій: знання (запам'ятовування ідей), розуміння (розуміння ідей), застосування (виконання ідей у реальному світі), аналіз (протиставлення та зв'язок ідей), синтез (об'єднання ідей) та оцінка (оцінка ідей). Учасники демонстрували "потенціал надмірної довіри до технології без належної перевірки", залишили критичне мислення ChatGPT замість того, щоб робити це самостійно та зміцнювати свої когнітивні здібності. Таким чином, потік інформації в час кліпового мислення та "розумних стрічок" новин сторінок соцмереж налагоджений мікротаргетинг створюють безальтернативну штучну реальність, в якій особстість не встигає відфільтровувати дані та будувати причинно-наслідкові зв'язки. Такі інструменти убезпечення від дезінформації як дебанкінг (спростування) та пребанкінг (попередні спростування) перестають ефективно діяти. Дебанкінг означає спростування того, що вже сталося, а пребанкінг — це дія на випередження, коли ми робимо заперечення заздалегідь. Обидві ці стратегії потребують побудови ефективної дорожньої карти викладу інформації на противагу, і якщо в цьому процесі не буде дзеркально використано технології ШІ, то всі зусилля захлинуться в масиві згенерованої неправдивої чи викривленої інформації, темпи поширення якої в десятки разів вищі за темпи випуску інформації традиційними медійними методами.

З огляду на експеримент Microsoft та Університету Карнегі-Меллона можна припустити, що оскільки використання ШІ знижує когнітивні здібності людини, а також її творчі можливості, то така згенерована інформація буде мати менший потенціал впливу, оскільки буде більш примітивною та менш креативно поданою. Відповідь на це припущення дав Майкл Томз, професор політології у Стенфордській школі гуманітарних наук і наук (Stanford School of Humanities and Sciences) та науковий співробітник Стенфордського

інституту штучного інтелекту, орієнтованого на людину (HAI) у своєму дослідженні [19]. На основі експерименту професор визначив, як впливає на респондентів дезінформація, згенерована трьома різними способами.

Перша група, контрольна, читала серію тезових тверджень, у які необхідно змусити людей вірити. Наприклад: "Більшість ударів дронів США на Близькому Сході були спрямовані проти мирного населення, а не терористів" або "Західні санкції спричинили дефіцит медичних товарів у Сирії". Оскільки ця група читала лише ці твердження без пов'язаної з ними пропаганди, вона стала відправною точкою для оцінки того, скільки людей вже вірить у ці твердження. Друга група учасників читала пропаганду, створену людьми, яка була написана на основі цих тезових тверджень і згодом викрита журналістами-розслідувачами або дослідниками. Третя група отримала пропагандистські матеріали на ті ж теми, що й перші дві групи, але створені великою мовною моделлю GPT-3.

Дослідники з'ясували, що приблизно чверть учасників контрольної групи погодилася з тезовими твердженнями, не читаючи жодної пропаганди. Пропаганда, написана людьми, підвищила цей показник до 47 %, а пропаганда, згенерована ШІ, — до 43 %. Коли ж матеріали, згенеровані ШІ пройшли редагування спеціалістами й було відкинуто ті статті, які не доносили потрібну думку, то було виявлено, що аж 53 % учасників погодилися з тезовими твердженнями після ознайомлення з пропагандою, що виявилося більш ефективним, ніж навіть пропаганда, написана виключно людьми.

Такий експеримент показав, наскільки впливовим є вдале використання ШІ в дезінформаційних кампаніях, хоч і негайні наслідки такої переконливої пропаганди не є очевидними. Коли ми беремо до уваги політичне поле битви когнітивної війни, особливо питання зовнішньої політики, то важливо пам'ятати, що люди можуть не мати глибоких знань або сформованої думки щодо них. Саме така таргет-група переважно стає основною для впливу ШІ-дезінформації. Ефективність автоматизованого написання пропаганди також звільняє людські ресурси для інших завдань у межах кампанії, наприклад, для створення фейкових акаунтів у соціальних мережах.

На підставі проаналізованого медіа середовища можна виокремити низку головних інструментів пропаганди та дезінформації як інструментів ведення когнітивної війни засобами штучного інтелекту, а саме: SMM-активності (Social Media Marketing); астротурфінг; дипфейк та підміна реальності; сугестія на сайтах державних структур тощо. Пропонуємо розглянути використання цих засобів дезінформації в рамках конкретних кейсів, реалізованих під час політичних, геополітичних протистоянь останнього десятиріччя, зокрема під час російсько-української війни.

SMM-активності (Social Media Marketing). З активним розвитком соціальних мереж з'явився ще один майданчик не тільки для продажу товарів, але й для продажу ідей. Інструменти соціального маркетингу в мережах мають чимало кейсів із використанням ШІ для управління свідомістю та вибором особистістю того чи іншого об'єкту. Серед основних принципів SMM,

якими послуговується інфлюенсори у когнітивній війні можна виокремити такі: соціальний доказ, обмін, емоційна пастка, прихильність, авторитетність, дефіцитність. Пропонуємо їх розглянути детальніше.

Принцип 1. Соціальний доказ. У його основі лежить підсвідома реакція людини на ситуацію, з якою вона не знайома. У разі відсутності в людини власного рішення чи досвіду, вона буде чинити, як більшість. У соціальних мережах, як і в класичних медіа, а також у політтехнології цей принцип успішно працює у вигляді рейтингів, відгуків, великої кількості лайків та перепостів, і не важливо, чи створені вони реальними людьми чи штучним інтелектом. Чим більше "користувачів" напише емоційний коментар з підтримкою дій влади — тим більше буде залучатися до підтримки доти нейтральних ідейно осіб; чим більше репостів навіть абсурдної новини — тим більший рівень довіри до неї тощо.

Принцип 2. Емоційна пастка. Між безособовою мережею та її користувачами налагоджується контакт "на ти", подібно клакеру в концертній залі, в більшості інтернет-дискусій присутній бот-тригер (переважно реальна особа, але останніми роками збільшилась кількість штучних аватарів), яка вчасно необхідними фразами та аргументами підживлює чи розпалю конфронтацію в діалозі. Таким чином цей механізм створює ефект того, що переможець онлайн-битв виграє не лише в мережі, але і в реальному світі. Адже коли люди починають вірити в нереальні події, то сила впливу таких вигаданих фактів на поведінку прирівнюється до сили впливу реальних.

Принцип 3. Прихильність. Ми любимо те, що нам подобається, і те, що на нас схоже, тому завдання ШІ — створити у публікаціях позитивні та схожі з портретом цільової аудиторії образи. Часто це блогери, які говорять спільною зі своїм читачем/глядачем мовою, використовують ті самі звороти та наративи, які не тільки підкреслюють їх приналежність до категорії "свій", але ще й закріплюють певні конструкти в свідомості реципієнта.

Принцип 4. Авторитетність. Рекомендація набуває особливої цінності, якщо вона дана експертом у своїй справі. Тому певні спільноти та блоги використовують у дописах аргументи відомих чи авторитетних у цій галузі людей, інколи навіть фейкових, але приписаних до певного професійного середовища. Повідомлення одразу набуває додаткової значущості та авторитетності.

Одним із найяскравіших прикладів участі лідера думки світового рівня у великій геополітичній грі в період широкомасштабної агресії РФ є вплив заяв і рішень Ілона Маска. Ще на початку війн компанія Маска SpaceX повідомила Пентагону, що відмовляється фінансувати служби супутникового зв'язку Starlink в Україні, проте згодом США взяли витрати на себе. Після купівлі бізнесменом компанії Telegram і її ребрендингу до соцмережі X в його руках опинилася колосальної потужності інформаційна платформа, яка дала можливість активно просувати не тільки наративи щодо України (часто антиукраїнські), але й завдяки їй стати де факто політичним гравцем в глобальному міжнародному полі, а з приходом до влади в США Дональда

Трампа, де юре. Після придбання Twitter Маск скоротив команди модерації та змінив політику платформи, що зробило менш ефективною боротьбу з фейковим контентом. Ця соціальна мережа — це багатомільйонна зброя масової маніпуляції в руках одного з найвагоміших інфлюенсорів сучасності, націлена як на внутрішню, так і на міжнародну аудиторію.

Варто заувжити, що Ілон Маск активно інтегрує штучний інтелект у соціальну мережу X через декілька ініціатив, що може мати кілька наслідків для поширення дезінформації. Упроваджений чат-бот Grok та інші ШІ-інструменти можуть значно прискорити створення та поширення дезінформації, оскільки вони здатні автоматично генерувати новини, які здаються правдоподібними, а також швидко адаптувати повідомлення під різні аудиторії, підсилюючи маніпулятивні наративи. У серпні 2024 року стало відомо, що платформа X використовувала дані користувачів для навчання моделей ШІ без їхньої явної згоди. Це викликало занепокоєння серед органів захисту даних у дев'яти європейських країнах, які подали скарги на X, звинувачуючи платформу у порушенні Загального регламенту про захист даних (GDPR). Таким чином, це дає нам можливість стверджувати, що таке явище, як персоналізована дезінформація, буде однією з головних загроз інформаційній безпеці найближчими роками.

Принцип 5. Дефіцитність. Таймери зворотного відліку на певні події, засилля конструктів, на кшталт "правда лише у нас", "у нас новини з'являються першими", "ми розкажемо те, про що змовчать інші" тощо підживлюють, як не абсурдно, фобію сучасної людини не отримати достатню кількість інформацію чи пропустити найголовніші гарячі новини. Саме внаслідок постійного інформаційного шуму формується відчуття дефіциту на умовно правдиву та гарячу інформацію, пропагандисти цим користуються, посилюючи це відчуття, "підсаджують" на голку своїх ресурсів у мережах. Особливо ефективно цей принцип спрацював під час побудови контент-планів безлічі Telegram-каналів, які почали активно з'являтися на початку широкомасштабного вторгнення РФ до України. Такі інформаційні канали стали прямими конкурентами загальнонаціонального марафону "Єдині новини", які були представлені державою, як основне джерело офіційної інформації. У цей час Telegram став платформою для максимально швидкого розповсюдження оперативної інформації в режимі реального часу, що не тільки часом шкодило безпеці цивільного населення, але й конфіденційності дій Збройних Сил України. Крім того засилля таких легкодоступних джерел інформації створює навколо особи інформаційний шум, який нашаровується на перманентний стресовий стан зокрема від масованих ракетних обстрілів території України, чим також провокував масову дезорганізацію та дезорієнтацію на фоні тотального стресу. Так, почали набувати неабиякої популярності Telegram-каналів, присвячені моніторингу повітряного простору України, які часом надавали фейкову інформацію та рекламували завдяки постам-клікбейтам так звані канали-сміттярки, під якими ховалась пропагандистська інформація. У травні 2024 року компанія OpenAI повідомила про виявлення

п’яти онлайн-кампаній у межах операції Doppelganger, які використовували технології генеративного ШІ для створення дописів у соціальних мережах, перекладу та редагування статей, написання заголовків з метою маніпулювання громадською думкою в усьому світі та впливу на геополітику [20].

Просто мати базу даних із соціально-демографічними характеристиками для формування цільової аудиторії пропаганди вже давно недостатньо. Після скандалу з Cambridge Analitica [21] Facebook з 2019 року обмежує доступ до даних про своїх користувачів навіть у рекламних кабінетах. Тому все більшої популярності набувають інструменти та кейси, які використовує SMM, зокрема ті, що сприяють підвищенню активності користувачів соціальних мереж, а саме змушують безпосередньо реагувати на пост через клік, репост, коментар тощо. Наприклад, такий спосіб комунікації з аудиторією, як флешмоб, не викликає жодної підозри у реципієнта, а відтак несе загрозу не тільки персональній безпеці кожного користувача соціальних мереже, але і національній безпеці в цілому, оскільки це прихованих спосіб формування і групування цільових аудиторій за її ключовими характеристиками з метою подальшого впливу на неї.

З огляду на те, в якому з таких флешмобів взяв участь користувач, він потрапляє до одного з сегментів, а разом з ним і всі ті, хто поставив “+” в коментарях до допису. Якщо у маніпуляторів немає якісних ШІ-парсерів (програм для збору даних користувачів), то наявність однакового тексту спрощує їм завдання. До того ж відразу формується база людей з мінімальною інформаційною гігієною, а вони підпадають під вплив маніпуляцій, фейків і пропаганди найлегше. Один з найбільш поширених флешмобів про нібито захист персональних даних дає можливість виокремити потенційних чи чинних конспірологів з мінімальним рівнем інформаційної гігієни.

Однак приховані методики формування цільових аудиторій з метою подальшого інформаційного впливу є сьогодні найменш дослідженими, хоч і набули неабияких масштабів. Крім того, вони, переважно, не потрапляють в коло визначених факторів, що впливають на інформаційну і національну безпеку. Проте саме на основі таких таргет-груп найчастіше відувається останнім часом навчання програм із ШІ, що дає можливість виявити лакуни інформаційної вразливості цільової аудиторії.

Астротурфінг. Сучасні кібертехнології дають можливість здійснювати сугестивний вплив не тільки завдяки різнорідному контенту, але й шляхом активного використання кіберсимулякрів — віртуальних акаунтів, які симулюють репрезентацію реальних людей і завдяки коментарям до певного інформаційного повідомлення можуть змінювати й деформувати його суть. У зв’язку з цим з’явився спеціальний термін астротурфінг. Активне використання новітніх інтернет-технологій сприяє заміщенню соціальної та політичної реальності комп’ютерними симуляціями [22].

У рамках антиукраїнської інформаційної кампанії керівництво РФ докладає зусиль для посилення ідеологічного, інформаційно-психологічного і пропагандистського впливу на населення України та окупованих територій,

зокрема використовуючи й астротурфінг. Свого часу історію астротурфінгу досліджували Ю. Данько [23] та Т. Паскаль [24]. Особливості астротурфінгу як одного із інструментів цифрової пропаганди РФ, а також його складових, що впливають на національну безпеку держави, досліджено недостатньо, оскільки більшість науковців зосереджували свою увагу саме на кібернетичних механізмах його творення, а також на як PR-технології та агресивного маркетингу.

Астротурфінг — це використання сучасного програмного забезпечення на основі ШІ та спеціально найнятих оплачуваних користувачів (так званих веб-бригад) для штучного управління громадською думкою. Ця технологія застосовується для витіснення думки реальних людей на веб-форумах, для організації підроблених кампаній в Інтернеті, які створюють враження, що велика кількість людей вимагають чогось конкретного, або виступають проти чого-небудь.

Термін походить від назви популярного бренду AstroTurf — синтетичного покриття, яке використовують замість трави на стадіонах. Згодом так стали називати процес створення штучної громадської думки, найчастіше в Інтернеті, в якому беруть участь спеціально найняті на фінансовій основі працівники на численних форумах, сайтах ЗМІ та в блогах. Вони пишуть замовні матеріали, залишають коментарі під постами в соціальних мережах або здійснюють масовий перепостинг необхідної інформації, створюючи таким чином враження спонтанної народної підтримки політика, політичної групи чи партії, продукту , сервісу, події тощо.

Оскільки астротурфінг є однією з форм кіберагресії, її здійснюють не тільки найняті користувачі (серед них можуть бути і так звані тролі — дійові особи, які надають експресивного забарвлення новинам), а й боти, фейкові акаунти, вбудовані банери прихованого рекламного змісту тощо, які створенні за допомогою ШІ. Троль — креативний, бот — механічний. Але аналіз сучасних підходів до генерації обох цих механізмів дає можливість стверджувати, що і той, і інший містить механізми функціонування ШІ, однак у різній мірі залучає до його використання людське управління (троль більшою мірою керується за безпосередньої участі людини). У сучасному інформаційному середовищі дедалі частіше застосовують комбінований підхід: бот + людина. Така формула є найбільш ефективною, оскільки людина, координуючи роботу бота, може максимально точно налаштувати його інформаційний вплив відповідно до конкретних завдань, мети та цільової аудиторії.

Термін астротурфінг у 1970-му році був застосований сенатором від штату Техас Ллойдом Бентсеном. У той час політик змагався з майбутнім президентом США Джорджем Бушем-старшим за місце в Сенаті США. Тоді команда Дж. Буша ініціювала народні рухи на підтримку республіканців. Виступаючи перед виборцями, Л. Бентсен назвав такі керовані групи штучною травичкою, а не справжніми рухами “від коренів, від ґрунту”. Термін також прижився в політології, втім, як і технологія створення штучних народних рухів [23].

Т. Паскаль відзначає, що астротурфери проводять збір підписів і розсилку листів, організовують пікети, мітинги та з'їзди і направляють делегації до політичних лідерів. І якщо у випадку традиційних громадських рухів ініціатива йде від самих людей, то в цьому — вона є політичним або комерційним проєктом, керованим PR-режисерами [24].

Із розвитком соціальних мереж робота астротурферів спростилася. Тепер для створення блогу чи мікроблогу не потрібно докладати великих зусиль, необхідно лише мати комп'ютер, доступ до Інтернету і вміння заповнити реєстраційну форму.

Ботоферми — humanware — це групи людей, що фізично працюють з великою кількістю ботів. Через спеціальні інтерфейси люди лайкають, коментують і поширюють інформацію з багатьох акаунтів й за це отримують невелику платню. Така взаємодія потрібна, аби обходити капчі — запобіжні заходи, що мають на меті відрізнити бота від справжньої людини [25]. Очевидно, що інформація, коментар, думка, отримані від комунікатора, близького за своїми характеристиками до реципієнта, мають значно вищий рівень довіри. Коли в інформаційному просторі є велика кількість таких віртуальних комунікаторів, виникає кумулятивний ефект, і простий користувач піддається потужній маніпулятивній атаці, вважаючи, що більшість таких же, як він, користувачів дотримуються певних поглядів і мають стійкі спільні цінності.

Так звані Ольгінські боти (ТОВ "Агентство інтернет-досліджень") з 2013 року в результаті викриття журналістами спеціально обладнаного для тролінгу офісу в Ольгіні, історичному районі Санкт-Петербурга, стали алегоричною назвою всієї російської системи бот-пропаганди. Їх також називать "фабрика тролів", "кремлеботи" — користувачі-провокатори, які за гроші у спеціально обладнаних офісах лишають дописи та коментарі під новинами інтернет-видань або на інших ресурсах в мережі з метою розповсюдження російської пропаганди в соціальних мережах, використовуючи технології ШІ, що значно ефективнішу автоматизує процес. Робота найнятих коментаторів, які розміщували неправдиву інформацію і провокативні коментарі, стала однією зі складових масштабної інформаційної війни Росії проти України, при чому алгоритми роботи астротурферів на кожному етапі війни набували нових масштабів та особливих характерних рис відповідно до запущених дезінформацій них кампаній. При цьому використовувалися не лише російські інтернет-ресурси, але й інтернет-ресурси України, Європи, США задля висвітлення подій з вигідної для російської пропаганди точки зору, або для формування громадської думки щодо них [26]. Саме такі офіси РФ використовує з метою активного астротурфінгу.

Крім того ще у 2015 році Росія оголосила про створення програмно-апаратного комплексу аналізу військовополітичної обстановки (ПАК ВПО) та аналізу суспільно-політичної, а також соціально-економічної ситуації в країні (ПАК ОПС). Її головна суть — це інтернет-розвідка, яка полягає у поданні посадовим особам міністерства оборони Росії інформації про най-

більш значущі події в країні та за кордоном, моделювання сценаріїв розвитку обстановки, підготовка пропозицій керівництву в автоматизованому режимі. Крім того, система моє розпізнавати зображення та здатна ідентифікувати людей та об'єкти. Комплекси також зчитуватимуть рядок, що біжить в ефірі ТБ-каналів, і обробляють радіосюжети [27]. Це підтверджує значущість цифрових технологій ШІ у розповсюджені та аналізі концептуальних конструктів, що в своїй сукупності відображають воєнно-політичну обстановку тієї чи іншої країни і забезпеченні національної безпеки. Завдяки такому програмному забезпеченню акумулюється актуальна інформація, досліджується цільова аудиторія, генерується базовий пул наративів для чергової хвилі астротурфінгу.

Головними функціями астротурфінгу є:

формування помилкового уявлення про події та явища, навіювання хибних спогадів тощо;

маніпулювання (створювання емоційних й інформаційних пасток, які впливають на прийняття рішень, вибір певної позиції тощо);

формування певного емоційного фону в аудиторії (почуття паніки, страху, байдужості тощо);

провокування ворожнечі та агресії (міжнаціональної, расової, релігійної тощо);

формування масової позаколективної поведінки (стимулювання до дій оффлайн). І якщо бот здебільшого механічно дублює задану алгоритмом інформацію, то троль створює інформаційні повідомлення, які містять емоційно-експресивну лексику та викликають почуття емпатії у реципієнта.

За даними дослідження Принстонського університету (США), Росія несе відповідальність за 72% операцій з дезінформації у світі, включно у соцмережах, обігнавши Китай, Іран і Саудівську Аравію [28]. Астротурфінг активно використовує Російська Федерація як частину гібридної війни з Україною ще з часів Революції Гідності. Послуговування астротурфінгом російською владою відрізняється від традиційних форм пропаганди. Її мета — не переконати чи довести, а підірвати та дискредитувати. За ступенем впливу його можна віднести до категорії зброї масового ураження, але не одномоментного, а прихованого, що прогресує як "інформаційна пандемія". Кремль активно використовує ботоферми з метою дестабілізації суспільно-політичного стану України та інших розвинених демократичних країнах.

Oxford Internet Institute, який є частиною Оксфордського університету, детально аналізує проблему кіберпропаганди в дев'яти різних країнах, зокрема й в Україні [29]. Учасники цього дослідження Сем Вуллі та Філ Говард стверджують, що після Євромайдану та анексії Криму Росією Україна перетворилася у фронт численних кампаній із дезінформації, більшість з яких має інтернет-компонент з активним використанням соціальних мереж, тролів і ботів, з чим пов'язана низка певних внутрішніх та зовнішніх загроз національній безпеці. Згідно з даними дослідження 21% українців використовують соціальні мережі як основне джерело новин, у той час,

коли будь-яка соціальна мережа може бути платформою для активного астротурфінгу, метою якого є дезінформація.

З початком російської агресії проти України у 2014 році ольгінські тролі активізувалися на просторах укрнету на різних платформа. До 2017 року, коли сталося блокування російської соцмережі "ВКонтакте" (VK) в Україні, вона була другим за популярністю сайтом після Google. З моменту захоплення Криму, з часів розгортання "руської весни" у східних і південних регіонах було створено багато груп з політичним забарвленням, що підтримували незаконні дії РФ на території нашої країни та поширювали антиукраїнську пропаганду. Серед найбільш відомих антиукраїнських груп тих років у VK можна виокремити такі [30]:

"Сводки от ополчения Новороссии" сумнозвісного Ігора Стрєлкова, який навесні 2014 керував операцією із захоплення Слов'янська, а під час широкомасштабної збройної агресії РФ з лютого 2022 року є активним YouTube-блогером з воєнно-політичних питань;

"АнтиМайдан" і ще велика кількість спільнот, які мають це слово у своїй назві;

"Народное ополчение Донбасса";

"Русская весна";

"Донецкая республіка" та безліч інших.

Vox Ukraine наприкінці 2018 року проаналізувала базу даних з майже 4 тисяч російських акаунтів, оприлюднених Twitter у жовтні того ж року. Було виявлено, що за період з 2010 по 2018 роки 1369 акаунтів російського "Агентства інтернет-досліджень" згенерували 774 957 твітів про Україну. Сумарна кількість фоловерів у цих профілів — 3,4 млн користувачів. До анексії Криму російські боти у Twitter майже не торкалися української тематики [31]. Поступовий сплеск активності у них почався після псевдореферендуму в Криму.

Одним із найяскравіших кейсів першого періоду російсько-української війни — активність у відповідь на катастрофу малайзійського Боїнгу MH17 авіакомпанії Malaysia Airlines, яка сталась на непідконтрольних територіях Донбасу 17 липня 2014 року і забрала життя 298 людей. За однією з "теорій змови" літак був збитий у повітрі українським винищувачем. Ця версія постала з Twitter-повідомлення іспанського авіадиспетчера Карлоса (@spainbuca), який нібито супроводжував політ цього рейсу. Указаний користувач повідомив не тільки про те, що спостерігав дві українські ракети коло літака за секунди до його збиття, але й публікував низку твітів про відповідальність України за катастрофу: "Київ відповідальний", "Нам в диспетчерській загрожують", "Поки у мене не забрали телефон і не розбили мені голову, ще раз: Київ збив літак".

Допис @spainbuca поширило багато користувачів, а потім медіакомпанії RT і TASS, а також інші російські новинні агентства. А в липні 2014 року ці повідомлення було використано на прес-конференції Міністерством оборони Росії. Міністерство інформаційної політики України згодом довело, що

цей Twitter-акаунт був ШІ-ботом, діяльність якого було активізовано під час Євромайдану, щоб розповсюджувати антиукраїнські гасла. У вересні 2016 року спільне міжнародне слідство довело, що Боїнг було збито з БУКу з території, контрольованої проросійськими сепаратистами. У кінці 2014 року аккаунт знову активували, але вже під іменем Людмила Лопатишкіна, що й надалі поширював антиукраїнську пропаганду та дезінформацію завдяки автоматизації генерації твітів характеру клікбейт.

Під час широкомасштабного вторгнення неодноразово ботоферми розповсюджували фейкові новини про біолабораторії в Україні або "звірства" українських військових спрямоване на дискредитацію опонентів. Так, згідно з аналізом компанії CASM Technology [32], яка досліджує дезінформацію в мережі, саме на 24 лютого припав пік реєстрації нових користувачів у Twitter, що може свідчити про організацію мережі. Також після 24 лютого у Twitter стали виходити в топ пости з хештегами #IStandWithPutin та #IStandWithRussia. Якщо звернути увагу на профілі, які роблять пости з такими хештегами, то можна зауважити, що більшість з них або були створені напередодні вторгнення в січні–лютому, або вже під час нього. При цьому користувальницька географія з напівпорожніми профілями — це країни Африки та Азії. Однак найбільш насиченим російськими міжнародними дезінформаційними кампаніями з використанням ШІ виявився 2024 рік, рік великої кількості виборів у всьому світі, прагнучи підірвати міжнародну підтримку України та дискредитувати демократичних противників. Так 2024 року Міністерство юстиції США заявило, що зірвало російську пропагандистську кампанію, яка використовувала фальшиві акаунти в соціальних мережах, створені за допомогою штучного інтелекту, для поширення дезінформації в США та інших країнах [33].

Ботоферма використовувала ШІ для створення профілів, які імітували американців у X, та публікувала повідомлення на підтримку війни Росії в Україні та інших прокремлівських наративів. Це було частиною затвердженого та фінансованого Кремлем проєкту, який курував російський розвідник. За даними Міністерства юстиції, саму ботоферму та програмне забезпечення ШІ, що її підтримувало, організував неназваний редактор RT, російського державного медіа. У той же час компанії Meta, власник Facebook, і OpenAI, розробник ChatGPT, заявили, що виявили кампанії іноземного впливу, зокрема деякі, пов'язані з Росією, які використовували ШІ для маніпулювання громадською думкою. Варто зважати й на таке, що згідно із дослідженням Джоша Гольдштейна щодо ШІ-дезінформації пропаганда, згенерована штучним інтелектом, може менше впливати на думки суспільства, коли йдеться, наприклад, про вибір кандидата на виборах у двопартійній системі, де більшість людей вже мають чітко сформовану позицію [19].

Ще раніше, 2022 року дослідниками з некомерційних організацій Qurium та EU DisinfoLab було викрито російську дезінформаційну кампанію "Doppelgänger" ("Двійник"), спрямовану на поширення фейкових новин через сайти, які імітують відомі медіа. Вона охоплювала щонаймен-

ше 10 європейських країн, зокрема Німеччину, Велику Британію та Чехію продовжує діяти й сьогодні [34]. Особливістю "Doppelgänger" є створення сайтів-двійників за допомогою ШІ, дизайн яких схожий на відомі медіа, такі як німецький Der Spiegel або британський The Guardian. На цих сайтах публікуються фейкові статті, які потім поширюються через соціальні мережі за допомогою фальшивих акаунтів. Метою кампанії є просування інтересів Кремля та поглиблення розбіжностей серед його супротивників, включаючи США та Західну Європу. За даними розслідування, проведеного німецькими медіа Süddeutsche Zeitung, NDR і WDR, а також естонським виданням Delfi, російська "Агенція соціального дизайну" (АСД) відіграє ключову роль у цій кампанії. АСД, яку очолює політтехнолог Ілля Гамбашидзе, використовує дезінформацію для дискредитації України та її західних союзників, просуваючи інтереси Росії. Ця агенція тісно співпрацює з адміністрацією президента Росії та залучена до кампанії "Doppelgänger".

У серпні 2023 року компанія Meta виявила нову фазу операції "Doppelgänger", спрямовану на припинення підтримки України міжнародними партнерами. Ця фаза включала створення сайтів, що імітують впливові медіа, такі як The Washington Post та Fox News, для розміщення фейкових публікацій, які дискредитують лідерів США та України.

У липні 2024 року дослідники повідомили, що російська дезінформаційна мережа використовує інфраструктуру в Європі для поширення фейкових новин. Європейські компанії, свідомо чи ні, надають свої послуги для цієї дезінформаційної операції, яка впливає на їхні власні країни [34].

У вересні 2024 року нове розслідування підтвердило, що Кремль систематично використовує дезінформацію як зброю. Дві афілійовані з Кремлем фірми в Москві розробляли масштабні кампанії з дезінформації, націлені на виборців у США, Німеччині, Франції, Україні та Ізраїлі. Ці кампанії мали на меті посіяти сумніви щодо ліберальних демократичних цінностей через поширення проросійських наративів [34].

Вищевикладене підтверджує активне використання ШІ Росією задля дезінформації в контексті когнітивної війни, а операція "Doppelgänger" є масштабною та добре організованою кампанією дезінформації, спрямованою на підрив демократичних інституцій та посилення впливу Росії на міжнародній арені.

Deepfake та підміна реальності. Епоха "глибоких" ШІ-підробок із множинністю реальностей створила матрицю з інформації, в якій особистість стає не лише споживачем, але й елементом цієї системи. Користувач світової павутини примножує кількість інтерпретацій, а завдяки сучасним цифровим технологіям може створювати й альтернативну реальність, яку одразу розпізнати як фейкову майже неможливо. Зважаючи на максимально швидке споживання інформації в наслідок кліпового мислення технологія "deepfake" стала продуктом технології штучного інтелекту (ШІ), що призвело до стрімкого поширення у світі підроблених відео- та аудіозаписів. Чим досконалішим стає ШІ, тим більш переконливо виглядають нові підробки.

Технологія дипфейків — ще один приклад, де генерація зображень та відео ґрунтується на поєднанні різних алгоритмічних архітектур, зокрема глибоких залишкових мереж, які можуть з приголомшливою точністю зчитувати рухи губ, синтезувати мову та симулювати вирази обличчя і рухи тіла [35].

Ця технологія поступово змінює правила гри в сфері політтехнологій та інформаційних війн. Дипфейк стає проблемою національної безпеки нового покоління. Створення підроблених новин, зловмисні обмани, зокрема компрометації знаменитостей, публічних осіб та знищення політичної репутації відбувається завдяки цій технології з найбільшою результативністю, оскільки у споживача часу на глибинний аналіз майже немає у швидкозмінному потоці інформації особливо в часи загострення соціальних настроїв. Можливості поширення інформації, та сама spreadability, про яку писав у 2013 році американський дослідник Генрі Дженкінс у книзі "Spreadable Media" [36], погано впливає на сприйняття та усвідомлення — користувач у середньому схильний натискати на кнопку "поділитися", не замислюючися і спираючися переважно на привабливість, віральність контенту, ніж на його достовірність. Тому дипфейк став справжньою шок-технологією, від якої поки що немає абсолютного захисту — лише критичне мислення та фактчекінг.

Сьогодні найбільше занепокоєння викликає розвиток саме аудіо- та візуального контенту, створеного штучним інтелектом — технології, яку на момент її появи було відносно легко виявити, але яка стрімко стає дедалі складнішою для відрізнення від реальності. Прфесор Майкл Томз висловлює занепокоєння в тому, що "дипфейки, ймовірно, більш переконливі, ніж текст, вони мають більше шансів стати вірусними та виглядають значно правдоподібніше, ніж окремий написаний абзацю. Я надзвичайно стурбований тим, що нас очікує у сфері відео та аудіо" [37].

На світовому ринку вже є чимало додатків, за допомогою яких будь-хто може зробити deepfake. Найвідоміші — Zao, DeepFaceLab, Deepfakes web β тощо. Програмний директор неприбуткової американської організації Witness Сем Грегорі зауважує, що deepfake часто використовують для дискредитації жінок-журналістів і громадських активістів. Однак відповідно до його спостереження політики почали часто використовувати deepfake як виправдання невдалим промовам чи кинутим ненароком фразам у публічному просторі, що викликали резонанс, і стверджують — "це deepfake", що відповідає фразі "це фейкові новини" [38].

Перший великий резонанс на політичному підґрунті ця фейкова технологія створила 2020 року. Ситуація стосувалася соціально-політичного руху "Extinction Rebellion" (Бельгія), як технологіями deepfake змусив свого прем'єр-міністра країни Софі Вільмес розповісти, що причина коронавірусу — екологічні проблеми. Не менш резонансним випадком стала підміна відео виступу спікера Палати представників США Ненсі Пелосі, на якому було додано ефект стану алкогольного сп'яніння промовиці. Це відео переглянуло в мережі понад 2,5 млн користувачів соціальних мереж. Проте най-

відомішим фейковим відео став сфальсифікований виступ Барака Обами, де він лайливо звертавсь до Дональда Трампа. Мільйони людей переглянули на YouTube слова президента, яких той ніколи не говорив. Ніякого скандалу не було, оскільки в кадрі з'явився режисер цього монтажу Джордан Піл, який пояснив, що цією творчою витівкою він спробував привернути увагу до цифрової дезінформації.

У квітні 2023 року Республіканський національний комітет США випустив 30-секундне відео, яке містило зображення, створені за допомогою штучного інтелекту, на яких президент Джо Байден і віце-президент Камала Гарріс святкують перемогу на виборах. Потім відео показало змодельовані сцени хаосу, включаючи вибухи в Тайвані, поліцію у тактичному спорядженні, що патрулює Сан-Франциско, наплив мігрантів на південному кордоні США і покинуті будівлі на Уолл-стріт. Ці фальшиві інциденти можуть потенційно призвести до міжнародних політичних чи військових ескалацій.

Росія наразі тільки освоює можливості цієї технології. Вже хрестоматійним прикладом глибинного фейку став випадок, коли у 2017 році Міноборони РФ опублікувало кілька постів у Твіттері та Фейсбуці, у яких містилося "незаперечне підтвердження" співпраці США з бойовиками угруповання "Ісламська держава" (ІДІЛ). Натомість — це був обрізаний скріншот з промо до мобільної гри "AC-130 Gunship Simulator", а також відео роботи ВПС Іраку по бойовиках ІДІЛ у 2016 році.

Від початку широкомасштабного вторгнення РФ в Україну Центр стратегічних досліджень та інформаційної безпеки у Facebook [39] попереджав громадян про можливу цифрову провокацію з боку Кремля — deepfake, в якому Володимир Зеленський оголосить капітуляцію країни. Мета такого відео — дезорієнтувати, посіяти паніку, почуття зневіри в громадян, деморалізувати спецслужби країни і схилити війська до складання зброї. Якщо такого сценарію не було реалізовано щодо президента, то технологію "deepfake" було успішно застосовано в червні 2022 року з метою дискредитації мера Києва Віталія Кличка. Відомо, що кілька європейських столиць, отримали з фальшивої поштової скриньки запити на спілкування з ним через додаток "ZOOM". Мери Берліна та Мадрида погодилися на розмову. Завдяки указаній технології, хакери використали зовнішність Кличка для переговорів. У виданні "Deutsche Welle" повідомлялося, що в розмові з бургомістеркою Берліна Франциской Ґіффай фейковий Кличко говорив про соціальні виплати для українських біженців і попросив вжити заходів щодо заохочення молодих хлопців повертатися в Україну воювати. Також співрозмовник попросив підтримати Київ порадою щодо проведення ЛГБТ-прайду [40]. Ця розмова містила типові кремлівські наративи, які вказують на російський слід у цій фейковій розмові. Але оскільки пропагандисти припустились грубої помилки — побудували розмову виняткову на конструктах, що викликають резонанс, а не зробили її більш емоційно-психологічно інтертекстуальною та сугестивною, вона була згодом піддана сумніву самою бургомістеркою. Варто зауважити, що це перший випадок використання

deepfake у живому онлайн-спілкуванні на високому міжнародному рівні, що впливає не тільки на репутацію політичної персони, але й всієї країни.

Узагальнення досвіду використання ворогом ШІ дає можливість покращувати способи використання нових технологій, когнітивні кампанії на основі технології ШІ стають все складніше ідентифікованими. Однією з таких стала інформаційна кампанія "Матрьошка", в якій використовувались як технології астротурфінгу так і дипфейк у вигляді відео контенту. Кампанія дезінформації "Матрьошка" — це складна операція, яка використовує тактику кількох рівнів обману, щоб приховати її справжні джерела та ввести аудиторію в оману. Назва походить від російських ляльок-матрьошок, оскільки стратегія передбачає створення серії взаємопов'язаних фальшивих наративів, які, здавалося б, походять від різних незалежних джерел, що підвищує їхню достовірність і охоплення.

Основна ідея вказаної тактики полягає в тому, що на перший погляд дезінформація здається доволі достовірною внаслідок використання численних підроблених акаунтів, сайтів або джерел. Ця тактика почала діяти в період Олімпійських ігор–2024 в Парижі і мала такі етапи:

1. *Фальшиві джерела*. Спочатку створюються фальшиві або маніпулятивні джерела, які виглядають як реальні новини або інтерв'ю.

2. *Підроблені репортажі*. Потім ці джерела або акаунти публікують "новини", що є вигаданими або перекрученими, але доволі правдоподібни. Часто в цій кампанії, як ніколи раніше в російській дезінформації, використовувались саме підроблені відео – дипфейки.

3. *Просування через інші рівні*. Інші акаунти чи сторінки можуть перепостити ці фейкові новини, що створює враження, ніби новина шириться з різних джерел, і це додає їй легітимності. Дезінформація адаптована для того, щоб резонувати з певними аудиторіями, часто використовуючи наявні соціальні розбіжності та політичні напруженості. Маніпулюючи інтересами та уподобаннями конкретних груп, кампанія намагається посилити свій вплив і викликати розбіжності

4. *Приховування організаторів*. Завдяки такій багаторівневій структурі важко відстежити, хто саме стоїть за поширенням дезінформації.

Щодо України ця кампанія торкнулась однієї з найболючіших тем сьогодення — теми українських біженців та їх підтримки за кордоном. "Матрьошка" використовувала deepfake відео для атак на українських біженців, зокрема неповнолітніх. Ці маніпулятивні відео мали на меті зобразити біженців у негативному світлі, провокуючи зменшення підтримки України і посиленяя напруженості серед приймаючих громад.

Найчастіше, коли йдеться про використанні ШІ в контексті когнітивних війн чи загалом гібридної війни експерти та науковці зосереджують увагу на кібербезпеці, насамперед захисті інформаційних систем та їх інфраструктури, тоді як питання захисту людей майже не обговорюється. Тому на нашу думку, важливо розпочати й поглибити глобальну дискусію щодо небезпек впливу ШІ на свідомість та когнітивні здібності особистості.

Адже ШІ, створені для ідентифікації фальшивого контенту, не достатньо ефективні. Такі країни, як Росія та Китай вже навчилися обходити ці алгоритми під час своїх когнітивних атак завдяки вдосконаленню технологічних рішень щодо створення дезінформаційних матеріалів. Системи штучного інтелекту та генеративного ШІ змінюють способи використання знань, експертизи та інформації, що матиме конкретні наслідки для збройних сил і стратегічного мислення, запобігання та стійкість залежатимуть від загальносуспільної відповіді. Тому для забезпечення національної безпеки ти когнітивної безпеки, зокрема населення України, необхідно розробити дорожню карту вдосконалення інформаційного захисту, яка буде включати наступні кроки:

1) впровадження багатосторонньої, спільної стратегії, яка передбачає активну участь громадянського суспільства, традиційних медіа, урядів і збройних сил, міжнародних організацій і цифрових корпорацій у протидії ШІ-дезіфнормації. Впровадження на державному рівні такого поняття як технопломатія — технологічна дипломатія, дасть можливість ефективно реалізовувати двосторонню співпрацю, створювати нові шляхи для діалогу урядів і технологічно індустрієї та координації їх зусиль щодо розслідувань втручання у вибори, поширення дезінформації та шкідливого контенту, кібербезпеки або збору електронних доказів для політичних розслідувань тощо;

2) чинні міжнародні правові доктрини не охоплюють низку наступальних інформаційних та когнітивних операцій та консцієнтальних операцій, а тим більше ШІ-дезінформації, оскільки вони не чітко кваліфікуються як прості випадки тероризації чи підбурювання до насильства, навіть якщо вони мають на меті знищити цілісність інформаційної екосистеми під час збройного конфлікту. Тому важливо вдосконалювати на законодавчому рівні нормативно правове забезпечення захисту наслення від когнітивних атак, зокрема із використанням ШІ. Поряд з тим постає необхідність нормативно-правового забезпечення регулювання використання штучного інтелекту в рамках державного інформаційного поля на основі міжнародних актів і доктрин, зокрема таких: Закону ЄС про штучний інтелект; Рамкової конвенції про штучний інтелект, права людини, демократію і верховенство права; Акту Європейського Союзу про штучний інтелект тощо;

3) побудова стратегії когнітивного захисту із урахуванням методів соціально-поведінкової науки, що передбачає наявність профільних спеціалістів із поведінкового здоров'я, зокрема у підрозділах Збройних Сил країни;

4) підвищення рівня медіаграмотності, (біо)технологічної грамотності, цифрової освіти серед цивільного населення, особливо серед маргіналізованих груп;

5) збільшення досліджень (а також їх фінансування), спрямованих на розуміння масштабу, обсягу та походження дезінформації, тенденцій і патернів, що стоять за нею, а також механізмів, які використовують зловмисники (як державні, так і недержавні) для організації своїх дій і посилення дезінформації.

З огляду на вищевикладене можна стверджувати, що нові технології розвиваються набагато швидше, ніж урядова політика, і часто підривають чинні правові та політичні рамки. Щоб забезпечити відповідальне використання ШІ та розробити правильні реакції на його можливі зловживання на ранніх етапах, необхідно налагодити міцніші зв'язки, партнерства та відкриті розмови між законодавцями, інженерами та дослідниками.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. McLuhan H. M. Media Research: Technology, Art and Communication (Critical Voices in Art, Theory and Culture). Taylor and Francis. 2014. 202 p.
2. NATO 2022 Strategic Concept. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.
3. NATO Allied Command Transformation, 2023. URL: https://scholar.google.com/scholar_lookup?journal=Cognitive%20Warfare%20Exploratory%20Concept.%20NATO%20Allied%20Command%20Transformation%20(ACT).%20Report%20No.:%20ACT/SPP/CNDV/TT-6700.&publication_year=2023&.
4. Kirby A. The Death of Postmodernism And Beyond // Philosophy Now. A magazine of ideas. Issue 58. 2006. URL: //philosophynow.org/issues/58/The_Death_of_Postmodernism_And_Beyond.
5. Metamoderna. URL: http://www.metamoderna.org.
6. Freinacht, H. (2017). *The Lis tening Society: A Metamodern Guide to Politics.* URL: https://www.amazon.com/Listening-Society-Metamodern-Politics-Guides/dp/8799973901.
7. Definition of post-truth in English. Oxford Dictionaries. Lexico Dictionaries. URL: https://www.lexico.com/en/definition/post-truth.
8. Velasco, Joseph. You are Cancelled. Conference: 1st Rupkatha International Open Conference on Recent Advances in Interdisciplinary Humanities, October 2020. Vol. 12. URL: https://rupkatha.com/V12/n5/ rioc1s21n2.pdf.
9. Face2Face: Real-time Face Capture and Reenactment of RGB Videos. URL: http://www.niessnerlab.org/papers/2016/1facetoface/thies2016face.pdf.
10. Newton C. Facebook's CEO on why the social network is becoming 'a metaverse company' URL: https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.
11. Arquilla J., Ronfeldt D. The Emergence of Noopolitik: Towards an American Information Strategy. RAND/MA-1033-05D. 1999. 102 pp.
12. World Economic Forum (2024). Global Risks 2024: Disinformation Tops Global Risks 2024 as Environmental Threats Intensify. URL: https://www.weforum.org/press/2024/01/global-risks-report-2024-press-release/.
13. Libicki M. What is information warfare? Washington: National Defense University Press, 1995. 104 p.
14. The Battle for the Mind: Understanding and Addressing Cognitive Warfare and its Emerging Technologies. URL: https://static.ie.edu/CGC/CGC_TheBattleofTheMind_2024.pdf.
15. The Challenge of AI-Enhanced Cognitive Warfare: A Call to Arms for a Cognitive Defense. URL: https://smallwarsjournal.com/2025/01/22/the-challenge-of-ai-enhanced-cognitive-warfare-a-call-to-arms-for-a-cognitive-defense/.

16. Hans W. A. Hanley, Zakir Durumeric. Machine-Made Media: Monitoring the Mobilization of Machine-Generated Articles on Misinformation and Mainstream News Websites. URL: https://arxiv.org/abs/2305.09820.
17. Elon Musk's X pushed a fake headline about Iran attacking Israel. X's AI chatbot Grok made it up. URL: https://mashable.com/article/elon-musk-x-twitter-ai-chatbot-grok-fake-news-trending-explore.
18. The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects From a Survey of Knowledge Workers. URL: https://www.microsoft.com/en-us/research/uploads/prod/2025/01/lee_2025_ai_critical_thinking_survey.pdf.
19. How persuasive is AI-generated propaganda? URL: https://academic.oup.com/pnasnexus/article/3/2/pgae034/7610937?login=false.
20. Doppelganger — Media clones serving Russian propaganda. URL: https://www.disinfo.eu/doppelganger/.
21. Скандал с Facebook и Cambridge Analytica. Что мы знаем. URL: https://www.bbc.com/russian/features-43475612 (дата звернення: 23.09.2022).
22. Свідерська О.І. Формування віртуального натовпу шляхом маніпуляції свідомості населення. *Гілея: науковий вісник*. 2019. Вип. 149 (№ 10). С. 62—66.
23. Данько Ю. А. Астротурфінг як інструмент віртуальної маніпуляції та політичної пропаганди в умовах інформаційної доби. Сучасне суспільство. 2015. Вип. 2(1). С. 38—49.
24. Паскаль Т. Игры на зеленой травке: Grassroots Vs. Astroturfing. URL: http://www.protektgroup.ru/articles/PR_11/p_11.htm.
25. Десять кроків від «Холодної війни» до ботів у соцмережах. https://internews.ua/opportunity/10-krokiv-vid-holodnoyi-vijni-do-botiv-u-socmerezhah?fbclid=IwAR3QBo_OP5DCejirIJ--5wljqGQKZ_L2b9auoRBWsPlY7LdcBjyOuK-ABAE.
26. Агентство интернет-исследований. URL: http://rucompromat.com/organizations/agentstvo_internet-issledovaniy.
27. В России придумали интернет-»разведку». URL: http://www.segodnya.ua/world/v-rossii-pridumali-internet-razvedku587983.html (дата звернення 14.09.2020)..
28. Shapiro J. Trends in Online Foreign Influence Efforts. URL: https://esoc.princeton.edu/files/trends-online-foreign-influence-efforts.
29. Computational Propaganda in Ukraine: Caught Between External Threats and Internal Challenges. URL: http://blogs.oii.ox.ac.uk/politicalbots/wpcontent/uploads/sites/89/2017/06/Comprop-Ukraine.pdf.
30. ВКонтакте. URL: https://vk.com.
31. Как российская "Фабрика троллей" пыталась влиять на повестку дня в Украине. Исследование 755 000 твитов. URL: https://voxukraine.org//longreads/twitter-database/index-ru.html
32. #IStandWithRussia #IStandWithPutin. Message-based Community Detection on Twitter. URL: https://files.casmtechnology.com/message-based-community-detection-on-twitter.pdf.
33. Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm. URL: https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners.

34. Russian disinformation network's infrastructure is spread across Europe, report says. URL: https://therecord.media/doppelganger-disinformation-infrastructure-european-companies.
35. Mubarak Rami et al. A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats. 2023. URL: https://doi.org/10.1109/ACCESS.2023.3344653.
36. Henry Jenkins, Sam Ford & Joshua Green. Spreadable Media: Creating Value and Meaning in a Networked Culture. New York, USA: New York University Press. 2013. 352 p.
37. The Disinformation Machine: How Susceptible Are We to AI Propaganda? URL: https://hai.stanford.edu/news/disinformation-machine-how-susceptible-are-we-ai-propaganda.
38. Researcher Explains Deepfake Videos. URL: https://www.youtube.com/watch?v=u2lX70U7N0c&t=88s&ab_channel=WIRED.
39. Уявіть, що бачите в телевізорі Володимира Зеленського… URL: https://www.facebook.com/protydiyadezinformatsiyi.cpd/posts/13115173610056
40. Розмова з "Кличком": мерка Берліна стала жертвою пранкерів. URL: https://www.dw.com/uk/rozmova-z-klychkom-merka-berlina-stala-zhertvoiu-prankeriv/a-62258579.

РОЗДІЛ 7
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТІ ТА НАУКОВОМУ АНАЛІЗІ

Іван ТКАЧ,
доктор економічних наук, професор

Кабінет Міністрів України у грудні 2021 року затвердив Концепцію розвитку штучного інтелекту в Україні до 2030 року, відповідно до якої передбачено: "впровадження технологій штучного інтелекту у сфері освіти, економіки, публічного управління, кібербезпеки, оборони та інших сферах для забезпечення довгострокової конкурентоспроможності України на міжнародному ринку" [1]. 9 грудня 2022 року Міністр освіти і науки України під час засідання Уряду презентував програму великої трансформації "Освіта 4.0: український світанок" [2], яка була підготовлена командою МОН України на основних засадах і принципах Плану відновлення України.

Освіта 4.0 — це концепція освіти, яка передбачає використання новітніх технологій для поліпшення якості процесу навчання та підготовки здобувачів освіти до життя в цифровому суспільстві. Вона базується на принципах гнучкості, індивідуалізації, колаборації та розширеного навчання. Метою освіти 4.0 є підготовка здобувачів освіти до цифрової економіки та роботизації праці, критично і творчо мислити, розвивати навички життєвого та професійного самовдосконалення.

Для реалізації Концепції освіти 4.0 необхідно забезпечити доступ здобувачів освіти до сучасних технологій, відповідної інфраструктури та належного педагогічного супроводу. До основних технологій, які використовуються в освіті 4.0, належать штучний інтелект, віртуальна реальність, інтернет речей, машинне навчання та інші.

Штучний інтелект має величезний потенціал у трансформації освіти та наукового аналізу, забезпечуючи нові підходи до персоналізації навчання, підвищення ефективності наукових досліджень і полегшення обробки великих даних.

Серед апологетів дослідження ШІ як науки й засобу трансформації кожного аспекту цивілізації, зокрема освіти й наукових пошуків, є: математик А. Тюрінг [3], який у 1950 році відзначив, що у машини відсутнє емоційне відчуття, провівши перший тест перевірки системи ШІ на інтелектуальність; А. Ньюелл, Г. Саймон та К. Шоу [4], котрі у 1955 році створили першу програму ШІ — "Логік-Теоретик"; професор Дж. Маккарті [5] — запропонував у 1956 році власний понятєвий кентавр ШІ під час конференції в Дартмутському коледжі, символізувавши народження нової наукової галузі, а пізніше, у 1963 році, розробив мову "LISP" ("List Processing"); Дж. Робінсон [6],

який у 1965 році запропонував метод резолюцій; Дж. Вейценбаум [7] — у 1966 році розробив першого чат-бота ELIZA, котрий міг імітувати діалог із психотерапевтом; Дж. Ланьє [8] наприкінці 1980-х рр. запропонував і популяризував термін "віртуальна реальність" як відчуття реальних образів, які генеруються комп'ютерною технікою; М. Амосов [9] — вважав, що вивчення проблеми штучного інтелекту базується на вивченні наук фізіології, психології, техніки та філософії; Дж. Хінтон [10], котрий у 2006 році разом із колегами запропонував підхід побудови глибших нейронних мереж, а також спосіб уникнути зникнення градієнта під час навчання; Ф. Фукуяма [11] — вивчаючи окремі аспекти ШІ зазначав, що він є однією із характеристик інформаційного суспільства; дослідник Дж. Джефферсон [3], котрий стверджував: штучний інтелект не може відчувати та не здатний до усвідомлення самого себе; А. Погореленко [12] наголошувала на розвитку ШІ у міжнародних відносинах та низка інших вітчизняних і закордонних науковців [13, 14, 15, 16, 17, 18, 19, 20].

Також різні аспекти впровадження й використання технологій ШІ в освітніх установах розглянуто у працях українських і зарубіжних учених, дослідників і практиків, які внесли вагомий внесок у розвиток методик використання ШІ в наукових дослідженнях, як у світовому масштабі (С. Баумер (C. Baumer), А. Карневал (A. Carnevale), Т. Корбет (T. Corbett), С. Думареск (C. Dumaresq), Х. Фірман (H. Firman), Х. Джанга (H. Jang), І. Каніаваті (I. Kaniawati), П. Корбел (P. Korbel), М Мелтон (M. Melton), Б. Седжат (B. Sejati), Г. Сікманн (G. Siekmann), М. Сонг (M. Song) та ін.), так і в Україні (В. Биков, О. Глазунова, І. Громова, М. Клименко, О. Коновал, Т. Крамаренко, О. Лисенко, Н. Мартинюк, М. Мар'єнко, Л. Полякова, С. Семеріков, А. Солодков, В. Терещенко, О. Фурман, Р. Халіков, А. Шевченко, М. Шишкіна, І. Юзвішин та ін.). Їхні дослідження та публікації сприяють розширенню наукового знання та застосуванню передових технологій для досягнення нових вершин у сфері використання ШІ.

У своїх працях науковці довели, що штучний інтелект — це не просто технологічний прорив, а справжня революція, що змінює наше сприйняття світу і перетворює усі сфери нашого життя, включаючи професійну освіту та наукові дослідження. Сучасні досягнення в галузі ШІ відкривають перед науковою спільнотою безмежні можливості.

Основні властивості штучного інтелекту є такими [21]:

Самонавчання: штучний інтелект може вдосконалювати свої здібності, збираючи та аналізуючи дані, здійснюючи прогнози та підбираючи найбільш оптимальні рішення.

Розуміння мови: штучний інтелект може розуміти людську мову та взаємодіяти з людьми, включаючи голосові та текстові команди.

Сенсорна сприйнятливість: штучний інтелект може збирати та аналізувати інформацію з різних джерел, включаючи зображення, звук та сенсорні дані.

Можливість прийняття рішень: штучний інтелект може приймати рішення на основі зібраної інформації та розуміння контексту.

Креативність: штучний інтелект може генерувати нові ідеї та рішення, які раніше не були знайдені.

Швидкість і точність: штучний інтелект шукає, аналізує, синтезує та створює нову інформацію майже миттєво.

Сьогодні українські вчені активно досліджують технології ШІ в освітньому процесі. Особливу увагу приділяють використанню технологій ШІ в процесі навчання та розвитку інноваційних підходів у різних галузях діяльності.

У наукових установах і закладах вищої освіти України створено наукові колективи, що здійснюють дослідження у сфері ШІ. Зокрема в Інституті кібернетики імені В. М. Глушкова НАН України, в Інституті проблем штучного інтелекту МОН України і НАН України, в Міжнародному науково-навчальному центрі інформаційних технологій та систем НАН України та МОН України, в Інституті проблем математичних машин і систем НАН України, в Київському національному університеті імені Тараса Шевченка, в Національному університеті "Львівська політехніка" та в інших закладах України колективи вже отримали низку вагомих фундаментальних і прикладних науково-технічних результатів.

Штучний інтелект став однією з ключових технологічних революцій XXI століття, що впливає на різні галузі життя, включаючи наукові дослідження. Використання ШІ в наукових дослідженнях надає безліч можливостей для поліпшення ефективності, точності та обсягу досліджень, що розширює горизонти наукового знання.

Проте потрібні подальші та ширші дослідження можливостей ШІ. Тому використання ШІ в сучасній освіті наразі має надзвичайну актуальність і потенціал для модернізації підготовки студентів. Ця інноваційна технологія створює нові можливості для підвищення ефективності та доступності освіти, проте водночас супроводжується серйозними викликами й загрозами, такими як соціальні та етичні питання, технічні виклики та багато інших.

7.1. Використання штучного інтелекту в освіті

Беззаперечним є факт того, що ШІ стрімко розвивається й проникає у всі сфери життя. Освіта не є винятком і за останні роки інтерес до застосування технологій ШІ у навчальному процесі лише зростає. Ці технології, що колись здавалися проявом наукової фантастики, сьогодні стають невіддільною частиною повсякденного життя та чинником значних змін у суспільстві. Вдосконалення технологій ШІ та їх впровадження у освітній процес є важливим кроком до створення ефективнішої та доступнішої, більш інноваційної й творчої системи освіти, що відповідає сучасним вимогам і викликам, а також визначає розвиток цієї системи у майбутньому. Оскільки ШІ швидко став потужним чинником модернізації та покращення якості навчання, актуальність його застосування в освіті стрімко зростає [22].

Сьогочасні переміни у розвитку постмодерного суспільства мають дещо стрибкоподібний характер унаслідок створення та імплементації технологій ШІ. Штучний інтелект виступає продуктом людської діяльності, який завдяки здатності виконання окремих функцій людини суттєво інтегрувався в різні галузі та сфери її соціальної взаємодії включно й з освітнім сектором, пропонуючи нові рішення для покращення навчання й викладання та визначаючи тим самим майбутнє суспільства. Завдяки ШІ соціум увійшов у нову епоху свого існування — інформаційну, яка окреслює економічний розвиток життя: завдяки сучасним технологіям змінюються процеси пізнання, а, відповідно, й буття людини, комунікація набуває нових своїх форм. Поряд із цими перемінами змінюється й освітній ландшафт, а точніше — процес отримання знань, у рамках цього порушуються питання *мобільності, ефективності, часу та простору*. Якщо порівняти інформаційні технології на початковому етапі їхнього становлення і з теперішнім станом, можна помітити переважаючу роль технологій, які визначають місце людини в соціальній структурі суспільства, а держави — в економічній системі. Розвиток наукоємних технологій став мотивом до створення ШІ та повномасштабного впровадження його в повсякденне життя людини. Відповідно, тепер *сектор вищої освіти* має відповідати актуальним запитам її користувачів у процесі отримання знань, переносячи весь матеріал у віртуальний світ, створений ШІ, з метою розроблення адаптивного, інклюзивного, гнучкого, персоналізованого та ефективного навчального середовища й глибинного розуміння поведінки, реакцій, емоцій здобувачів освіти [23]. Заклади вищої освіти, які продукують освітні послуги, повинні здійснювати адаптацію власної стратегії розвитку та зосереджуватися на пропагуванні відповідального, якісного, етичного й прозорого використання інструментів ШІ своїми співробітниками та здобувачами вищої освіти відповідно до чинного законодавства з подальшим нівелюванням негативних наслідків його впливу на суспільство, культуру та економіку.

Загалом, еволюція розвитку навчання за допомогою інформаційних технологій датується ще початком 1980-х років і публікацією у 1989 р. першого Міжнародного журналу штучного інтелекту в освіті, тоді як Міжнародне товариство штучного інтелекту в освіті було засновано лише у 1993 р.

Фактично можна констатувати, що тема ШІ у сфері освіти пов'язана з його величезним світовим науковим потенціалом, який щоденно зростає, а розкриття її сутності чекає практичного розв'язання. Відповідно до цього, сьогодні активно здійснюється:

оприлюднення значного масиву наукових публікацій;

упровадження системи розпізнавання тексту;

відбувається реалізація програм персоналізованого та адаптивного навчання, що передбачає коригування змісту освіти в межах окремих освітніх компонентів на основі аналізу навчальних досягнень здобувачів освіти;

набирає актуальності прогнозна аналітика, інтервальне навчання, автоматичне оцінювання навчальних досягнень з можливістю аналізу відповідей та надання персоналізованої допомоги;

штучний інтелект застосовується у воєнній сфері (розвідка та аналіз даних; автономні бойові системи; кібербезпека та інформаційні війни; управління військовими операціями; медична підтримка та реабілітація; моделювання та навчання військових та інше);

застосовуються віртуальні помічники студентів — чат-боти (ChatGPT, Duolingo, Thinkster, Querium, Alta by Knewton та ін.).

За останні роки з'явилося багато інструментів, які змінюють життя як викладачів, так і здобувачів освіти, забезпечуючи зручність під час отримання знань. До прикладу, Google Translate дає можливість перекладати текст понад 100 мовами; Siri й Google Assistant — дають можливість людям ставити запитання та отримувати швидкі відповіді; ChatGPT — надає допомогу в наукових дослідженнях, підсумовуючи джерела чи скеровуючи до корисних публікацій, а також миттєві відповіді на будь-які запитання, пояснення, наведення прикладів, написання віршів чи оповідань; Stable Diffusion та Imagen — дають можливість вводити текст для створення реалістичних зображень; Caktus — надає персоналізовані рекомендації здобувачу освіти щодо контролю його навчання; Gradescope — допомагає викладачам швидше та ефективніше оцінювати завдання здобувача освіти, зменшуючи при цьому їхню упередженість; Alta by Knewton — дає можливість адаптовуватися до унікального стилю навчання кожного здобувача вищої освіти; Querium — імітує досвід викладача для орієнтації здобувача освіти до розв'язання проблеми завдяки використанню унікальної технології StepWise; Educationcopilot — пропонує зекономити час і енергію викладачів завдяки швидкому генеруванню індивідуальних шаблонів, а також надає можливість співпраці між викладачами та ін.

Штучний інтелект в освіті — це революційний спосіб допомоги здобувачам освіти у навчанні та наукових дослідженнях, який змінює процес отримання ними знань, доступу до інформації та навчальних ресурсів, допомагає раціонально використовувати час і долати простір, дозволяє навчатися у власному темпі, надає можливість отримання зауважень щодо слабких сторін, але водночас має чимало невивчених проблемних аспектів. Відповідно, варто зупинитися на виокремленні та детальному аналізі ключових переваг і негативних сторін використання ШІ в освіті й наукових пошуках здобувачів вищої школи. Аналіз наукових джерел дав можливість виділити основні переваги застосування технологій ШІ належать:

1. Системи ШІ вміють адаптуватися до навчальних потреб кожного здобувача та цілей відповідно до їх сильних і слабких сторін, успішності й поведінки, продукуючи тим самим персоналізоване навчання на варіативній основі.

2. Технології ШІ можуть аналізувати та спостерігати за поточним стилем навчання і наявними здібностями здобувача освіти, а також надавати налаштований шаблон вмісту їх підтримки.

3. Системи ШІ дають можливість оцінювати не лише закриті відповіді у тестовому форматі, але й описові.

4. Завдяки ШІ здобувачі освіти не соромляться робити помилки, що є невіддільною частиною їхнього навчання, оскільки потім отримують зворотний зв'язок у реальному часі для внесення необхідних виправлень.

5. Штучний інтелект може надавати здобувачам освіти доступ до освіти відповідно до їхніх потреб, наприклад, шляхом читання змісту особі з вадами зору або ж використовуючи голосовий зв'язок для глухих і слабочуючих студентів.

6. Технології ШІ можуть підтримувати оцифрування контенту, полегшуючи тим самим вилучення і використання потрібної інформації.

7. Делегування ШІ рутини (створення чернеток лекцій, завдань, систем для автоматизації оцінювання робіт, експрес-відповіді на поширені запитання, загальні відповіді на питання щодо написання, наприклад, курсового проєкту), надає змогу пришвидшити й розвантажити роботу викладачів.

8. Використання викладачами закладів вищої освіти переваг ШІ сприяє розширенню аудиторії для отримання знань без географічних обмежень і створенню нового іміджу освітянина.

9. Навчально-психологічна підтримка здобувачів освіти в опрацюванні знань, вмінь і навичок, формуванні нових компетенцій з допомогою технологій ШІ. Особливий наголос робиться на допомозі індивідуумам, які мають труднощі з навчанням, а також тим, хто має особливі потреби (інклюзивний підхід). Підтримка містить додаткові ресурси, пояснення та підказки [22].

Технології ШІ, маючи значні потенціали для ампліфікації сфери освіти та вдосконалення навчальних процесів, суттєво впливають на розвиток сучасної педагогіки та психології навчання. На основі ШІ розвиваються нові інструменти та підходи, що спрощують навчання, роблять його доступнішим і підвищують ефективність. Активно впроваджуються навчальні можливості нейромереж та сучасних освітніх платформ, побудованих на основі інформаційно-комунікаційних технологій (ІКТ) із залученням ШІ, таких як IBM Watson Education, SMART Learning Suite, Cognii, ChatGPT, DreamBox Learning Midjourney тощо. Вони забезпечують інструменти для організації та керування індивідуальним навчанням, зокрема аналітику даних, побудову персоналізованих навчальних програм, застосування інтерактивних віртуальних помічників, впровадження програм і застосунків для оцінювання знань, вмінь і навичок тощо. При цьому перспективним напрямом досліджень залишається вивчення того, як забезпечити достатній рівень знань і цифрової компетентності, щоб здобувачі освіти могли самостійно, етично й продуктивно працювати зі ШІ [24; 25].

Таким чином, впровадження технологій ШІ в освіту відкриває нові можливості для індивідуалізації навчання, підвищення його ефективності та доступності. Використання ШІ сприяє розвантаженню викладачів від рутинних завдань, даючи їм можливість зосередитися на творчому та інтерактивному складниках освітнього процесу, зокрема в умовах повномасштабної війни з російськими агресорами. Подальший розвиток ШІ в освіті передбачає вдосконалення його інструментів для автоматизації, адаптивного навчання,

надання персоналізованого зворотного зв'язку та навчально-психологічної підтримки. Інклюзивний підхід до навчання із залученням ШІ може значно покращити доступ до якісної освіти для здобувачів освіти з особливими потребами. Водночас перспективними напрямами досліджень залишаються розробка етичних стандартів, підвищення цифрової грамотності та розуміння принципів роботи ШІ серед освітян та здобувачів освіти. У цілому технології ШІ стають не лише важливим інструментом для вдосконалення сучасної освіти, а й основою для створення нових навчальних підходів, що можуть радикально змінити майбутнє педагогіки та психології навчання [22].

Проаналізувавши наявні публікації [26, 27, 28, 29, 30, 31, 32] та власний досвід використання ШІ, виокремлюємо такі можливості використання ШІ в освіті:

Індивідуалізоване навчання. Однією з ключових можливостей ШІ є можливість створювати індивідуалізовані навчальні програми для майбутніх педагогів. Алгоритми спроможні аналізувати вміння та слабкі сторони студентів і розробляти навчальні матеріали, які належним чином відповідають їхнім потребам. Це сприяє підвищенню ефективності навчання.

Аналіз успішності. Інструменти ШІ здатні аналізувати виконання студентами завдань і відстежувати їхній академічний прогрес. Вони можуть ідентифікувати студентів, які потребують додаткової підтримки, та надавати викладачам рекомендації щодо індивідуального підходу до кожного студента.

Віртуальні педагогічні симулятори. ШІ дає можливість створювати віртуальні педагогічні симулятори, де майбутні педагоги можуть відпрацьовувати навички в різних педагогічних ситуаціях. Це надає можливість отримувати практичний досвід і розвивати навички без необхідності проведення реальних занять. Чат-боти та віртуальні асистенти, побудовані на основі ШІ, стають важливими інструментами в освіті для взаємодії з студентами. Вони використовуються для відповіді на запитання, організації навчальних процесів, а також для підтримки навчальної мотивації студентів [33, 34]. Наприклад, в рамках дистанційного навчання системи на базі ШІ дозволяють забезпечити доступність навчальних матеріалів у реальному часі.

Автоматизація адміністративних завдань. Технологія ШІ може автоматизувати безліч адміністративних завдань, включаючи створення розкладів, облік результатів навчання студентів і ведення документації. Це дозволяє вчителям чи викладачам витрачати менше часу на рутинні завдання та більше часу — на навчання та взаємодію зі студентами.

Підвищення якості викладання. ШІ може аналізувати та вдосконалювати якість викладання, надаючи викладачам зворотний зв'язок щодо їхніх методик і підходів, допомагаючи вдосконалити процес навчання.

Глобальна співпраця. За допомогою ШІ студенти та викладачі можуть співпрацювати та обмінюватися досвідом з колегами з усього світу. Це створює можливість для більш глибокого розуміння міжнародних педагогічних практик і підвищення культурної освіченості.

Ефективність і доступність. Використання ШІ може підвищити ефективність і доступність педагогічної підготовки. Онлайн-ресурси, чат-боти для освітньої підтримки, відкриті курси та платформи для дистанційного навчання стають усе більш доступними і дозволяють педагогічним закладам освіти залучати студентів з різних частин світу.

Створення інноваційних навчальних матеріалів. ШІ може генерувати інноваційні інтегровані навчальні матеріали, такі як інтерактивні уроки, мультимедійні презентації та відеокурси. Це робить навчання більш захоплюючим і ефективним, сприяючи активному залученню студентів.

Підготовка до цифрової реальності. Використання ШІ допомагає майбутнім педагогам оволодіти цифровими навичками та адаптуватися до світу технологій, які швидко змінюються. Вони стають більш компетентними у використанні цифрових інструментів у навчальному процесі.

Постійне вдосконалення. ШІ дає можливість студентам і викладачам здійснювати постійне вдосконалення, отримуючи доступ до оновлених матеріалів і ресурсів у реальному часі. Це важливо в умовах постійних змін у сфері освіти та педагогіки.

Поряд із цими перевагами, є *низка серйозних проблем*, які суперечать якісному та стабільному застосовуванню технологій в освітній діяльності:

відсутність (недосконалість) законодавчо-нормативного регулювання використання ШІ в усіх видах діяльності;

питання конфіденційності й безпеки даних;

зниження когнітивних здібностей як серед здобувачів освіти, так і серед викладачів; ризик надмірного повсякденного використання технологій (ШІ слід розглядати лише як доповнення до навчальних матеріалів, розроблених викладачем);

відсутність посилань на джерела інформації;

упередження в даних і алгоритмах;

зазіхання на інтелектуальну власність і авторське право;

ризик отримання неправдивої інформації, оскільки ШІ часто генерує текст, наповнений “водою”;

шахрайство в навчанні, що призведе до значного зниження рівня знань і навичок цілих поколінь;

адаптація системи освіти: ШІ є серйозним викликом для освітнього й наукового простору, якщо система не зможе швидко пристосуватися до реальності.

Можливості використання ШІ в підготовці здобувачів вищої освіти дійсно вражають своєю різноманітністю та потенціалом для поліпшення якості навчання та розвитку освіти. Проте необхідно пам’ятати про *етичні аспекти* використання цих технологій, а також про постійний моніторинг і вдосконалення їхнього впровадження в освітньому процесі. Тому науковці [35, 36, 37] звертають увагу на такі загрози використання ШІ в освітній діяльності:

Втрата людського контакту. Занадто широке використання технологій і ШІ може призвести до втрати людського контакту у навчанні. Наприклад,

педагогічна підготовка передбачає взаємодію та спілкування, і надмірне використання комп'ютерів та інших пристроїв може вплинути на розвиток міжособистісних навичок та емоційного інтелекту студентів.

Приватність даних. Збір та обробка великих обсягів особистих даних може порушити приватність студентів і викладачів. Важливо забезпечити надійний захист даних і дотримання вимог законодавства про захист приватності.

Залежність від технології. Інтенсивне використання ШІ може зробити педагогічну систему вразливою до технічних збоїв або відмов. Важливо мати альтернативні навчальні підходи та плани на випадок непередбачених ситуацій.

Відсутність етичних норм. Беручи до уваги швидкі технологічні зміни, може виникнути відсутність чітких етичних норм щодо використання ШІ в педагогічній підготовці. Необхідно розробляти та дотримуватися етичних стандартів для забезпечення справедливого та етичного використання технологій.

Нерівність доступу. Нерівність у доступі до технологій може стати проблемою, оскільки не всі студенти та навчальні заклади мають однаковий рівень доступу до інноваційних ресурсів. Це може створити нерівні умови для навчання.

Витрати на впровадження та підтримку. Впровадження та підтримка систем ШІ вимагають великих фінансових ресурсів. Заклади вищої освіти повинні бути готові інвестувати у витрати на придбання, налаштування та підтримку цих технологій. Недостатнє фінансування може стати перешкодою в успішному впровадженні ШІ в підготовку здобувачів освіти.

Заходи безпеки та кіберзагрози. Використання ШІ підвищує вразливість до кібератак та злому. Важливо вживати заходи безпеки, щоб захистити навчальні системи від потенційних загроз.

Втрата робочих місць. Автоматизація та впровадження ШІ може призвести до автоматизації ряду педагогічних завдань, що може вплинути на кількість робочих місць в закладах освіти. Важливо розглядати аспекти соціального впливу впровадження технологій на робочу силу.

Супровід та навчання. Інтеграція ШІ вимагає спеціалізованого супроводу та навчання для викладачів і студентів. Недостатній рівень підготовки може призвести до неефективного використання технологій та недоліків у їхньому впровадженні.

Загрози використання ШІ в підготовці здобувачів освіти вимагають уважного розгляду та вжиття заходів для їхнього вирішення. Це може бути досягнуто за допомогою ретельного планування, розроблення етичних стандартів та інноваційних підходів до навчання та викладання. Беручи до уваги як можливості, так і загрози використання ШІ в освітній діяльності, важливо забезпечити баланс та ефективне використання цих технологій для досягнення найкращих результатів у сфері освіти.

Враховуючи зазначені переваги та проблеми процесу імплементації технологій ШІ в освітню складову та науково-дослідну діяльність здобувачів

вищої освіти, вважаємо, що така трансформація є важливою компонентою переходу до нового типу освітнього процесу з інтеграцією різних галузей науки, реформуванням організації науки й пізнавального процесу в ній, що передбачає володіння практичними навичками опрацювання інформації з використанням технологій ШІ, користування електронними бібліотеками та наукометричними базами, засобами аналізу даних досліджень, застосування досвіду ефективної роботи з електронними документами іншомовного походження тощо. Сьогодні в процесі наукового пізнання студентами відбувається виключення людського мислення, дослідження протікає ніби в автоматичному режимі або ж взагалі без безпосередньої його участі — відбувається радикальна трансформація характеристик обізнаності, умінь і мислення здобувача вищої освіти, а також експериментальної бази наукових досліджень. Практичне застосування технологій ШІ допомагає здобувачам освіти зекономити час, який є вкрай необхідним для збирання важливих повідомлень, що швидко стимулює його творчу результативність, евристичність пошуку, поетапну та загальну продуктивність праці.

Адекватне, етичне й розумне використання технологій ШІ здобувачами вищої освіти в освітньому процесі й наукових пошуках провокує появу іншого світу з новим освітнім ландшафтом, алгоритмами розвитку цивілізації, а також новими індивідуальними, соціальними й наукоємними технологіями. Сучасна реальність здобувача освіти вже є неможливою без щоденного застосування ШІ, оскільки пропоновані технології мають вже зовсім не другорядну роль, а несуть важливе концептуальне й методологічне значення [20].

Поряд з цим, що використання ШІ в освітньому процесі та безперервному навчанні, отримало широке застосування, існують важливі аспекти, що залишаються недостатньо розкритими як у середній так і вищій освіті. Зокрема, питання персоналізації освітнього процесу більшою мірою розглянуто, але певні обмеження щодо її впровадження на практиці потребують додаткової уваги [38].

Одним з аспектів, який потребує подальшого дослідження, є застосування ШІ для індивідуального аналізу потреб здобувачів освіти. Незважаючи на великий потенціал таких технологій, їх широке впровадження в закладах освіти стримується практичними та теоретичними обмеженнями.

Крім того, значним викликом залишається відсутність великих обсягів даних, які могли би підтвердити ефективність використання ШІ в контексті безперервного навчання. Достеменно відомо, що є короткострокові переваги, як-от підвищення залученості здобувачів освіти та надання індивідуалізованого досвіду навчання, однак недостатньо даних щодо довгострокових наслідків впливу ШІ на критичне мислення і загальну продуктивність здобувачів освіти [39]. Для розв'язання цієї проблеми необхідно проводити додаткові дослідження, спрямовані на вивчення впливу технологій ШІ на різні освітні середовища та типи здобувачів освіти [40].

Крім того, етичні питання залишаються одним із найбільших викликів у сфері використання ШІ. Наприклад, упередженість алгоритмів викликає

серйозне занепокоєння, оскільки системи ШІ ґрунтуються на даних, що можуть містити структурні упередження. Як показують дослідження, в руках неетичних осіб такі технології можуть призвести до освітньої нерівності, оскільки алгоритми ШІ можуть відтворювати ці упередження [41]. Проблема конфіденційності даних також є перешкодою на шляху до широкомасштабного впровадження технологій ШІ.

Хоча нині є чітке розуміння потенціалу ШІ в персоналізації освітніх процесів, його повне впровадження в системи освіти різних країн залишається недостатньо дослідженим. Необхідно детальніше вивчити, як ці технології можуть бути адаптовані до специфічних освітніх середовищ з урахуванням культурних та соціальних факторів.

Також важливим питанням є вплив штучного інтелекту на довгострокову ефективність освіти [42]. Натепер більшість досліджень сфокусовано на короткострокових результатах, таких як підвищення залученості та покращення успішності здобувачів освіти, проте питання, як ці технології впливають на розвиток критичного мислення, творчості та глибоке розуміння матеріалу у довгостроковій перспективі, залишаються відкритими. Отже, дослідження спрямовано на вивчення цих невирішених питань, зокрема щодо впливу штучного інтелекту на довгострокові освітні результати, адаптації технологій до різних культурних контекстів і розроблення етичних стандартів для їх безпечного й ефективного використання.

За останні роки за допомогою ШІ в освіті з'явилися різноманітні засоби індивідуалізованого навчання. Деякі з них включають машинне навчання, оброблення природної мови, інтелектуальні системи навчання та адаптивні системи навчання, які ефективно налаштовують навчання відповідно до можливостей кожного здобувача освіти [40].

Машинне навчання та прогнозну аналітику можна визначити як процес використання розширених алгоритмів і статистичних моделей для аналізу великої кількості даних і точного прогнозування щодо деяких подій чи ситуацій на основі подібних подій чи ситуацій у минулому.

Алгоритми навчання під наглядом беруть участь в аналізі моделей поведінки здобувачів освіти, а також моделей успішності. Досліджуючи велику кількість даних, такі алгоритми здатні знаходити закономірності у взаємодії здобувачів освіти з наповненням, труднощі, з якими вони стикаються, та їхні успішні стратегії навчання. Це дає змогу розробити модель здобувачів освіти, яка передбачить майбутні результати учасників освітнього процесу, щоб можна було вжити відповідних заходів. Наприклад, Coursera та інші інструменти EdTech намагаються передбачити результати здобувачів освіти на основі даних їх взаємодії та рекомендують відповідні матеріали і вправи для кожного зі здобувачів [43].

Завдяки обробленню природної мови (ОПМ) взаємодія ШІ зі здобувачами освіти є унікальною, особливо в розділах вивчення мови та письма. Одним із корисних застосувань систем, заснованих на ОПМ, є надання здобувачам освіти письмового відгуку про їхні роботи, включаючи помил-

ки в граматиці та стилі, а також сильні та слабкі сторони їхніх аргументів. Крім того, такі програми ШІ, як програми для перевірки граматики, а саме Grammarly, і для вивчення мов, як-от Duolingo, використовують ОПМ для врахування диференційованих здібностей здобувачів освіти, при цьому рівень складності матеріалу, який їм надається, однаково відповідний. Той факт, що зворотний зв'язок та інструкції надаються відповідно до рівня компетенції та стилю навчання користувача, робить процес навчання більш ефективним і відповідним його потребам [40].

Інтелектуальні системи навчання (ІСН) пропонують інший підхід до персоналізації, забезпечуючи реальне, адаптивне навчання. Ці системи адаптують спосіб, який допомагає здобувачу освіти вирішити проблему, беручи до уваги вхідні дані здобувачів освіти та надаючи додаткові підказки або розроблені кроки, якщо потрібно. Ця стратегія навчання була дуже корисною в таких сферах, як математика, природничі науки та інші курси, де широко використовуються блок-схеми або алгоритми [44]. Деякі з них включають MATHia від Carnegie Learning, де здобувачі освіти можуть ознайомитися з предметом із правильною швидкістю, програма завжди буде складною, але не неможливою для освоєння, оскільки вона передбачає розрізнення рівня складності для кожного здобувача освіти.

Адаптивні навчальні платформи є прикладом високорівневого застосування диференційованого навчання, оскільки система постійно модифікує освітній контент відповідно до прогресу здобувачів освіти. Зокрема, такі програми, як DreamBox і Knewton, інтегрують функції штучного інтелекту, що дозволяють у режимі реального часу контролювати освітній процес. Вони адаптують навчальні матеріали до індивідуальних особливостей здобувачів освіти: поглиблюють зміст у разі виникнення труднощів або підвищують рівень складності за демонстрації здобувачами високих результатів.

Ці платформи є ефективними інструментами для різних освітніх рівнів — від початкових шкіл до університетів, забезпечуючи індивідуальні траєкторії навчання, що сприяє підтримці мотивації здобувачів освіти та забезпечує безперервний навчальний прогрес. Дослідження свідчать, що інтеграція адаптивних систем у викладацький процес підвищує ефективність навчання завдяки створенню гнучкого та індивідуалізованого освітнього середовища, яке враховує потреби кожного здобувача освіти [32].

Отже, в сучасних освітніх технологіях ШІ є вирішальним компонентом, який включає *машинне навчання*, *оброблення природної мови*, *інтелектуальні системи навчання* та *адаптивні навчальні платформи*. Така інтеграція технологій створює міцну основу для диференційованого навчання, яке стає *індивідуалізованим*, *гнучким* і *ефективним*. Застосовуючи ШІ для підтримки освітніх процесів, викладачі мають змогу більш ефективно задовольняти різноманітні навчальні потреби здобувачів освіти, що сприяє їх активній участі в освітньому процесі та досягненню вищих результатів. Штучний інтелект активно використовується в навчальних системах для покращення диференційованого підходу до навчання, зокрема з урахуванням індивіду-

альних потреб кожного здобувача освіти. У таблиці 7.1 надано перелік реальних прикладів застосування технологій ШІ різними компаніями та платформами для забезпечення персоналізованого навчання.

Таблиця 7.1. **Приклади успішного впровадження штучного інтелекту в диференційоване навчання**

№ з/п	Практичний приклад	Успішне впровадження штучного інтелекту компанією в диференційоване навчання	Вплив на здобувачів освіти і викладачів
1.	Carnegie Learning	Платформа MATHia від Carnegie Learning використовує штучний інтелект для надання персоналізованих інструкцій з математики, адаптації до індивідуальних відповідей здобувачів освіти в режимі реального часу, щоб запропонувати цілеспрямовану практику та зворотний зв'язок	*Здобувачі освіти*: збільшення залученості та розуміння завдяки покроковому розв'язанню проблем. *Педагоги*: зменшення навантаження за допомогою автоматичного відстеження прогресу здобувачів освіти й індивідуальних планів уроків
2.	DreamBox Learning	DreamBox пропонує адаптивну навчальну платформу для математики K-8, яка динамічно регулює складність уроків на основі успішності здобувачів освіти відповідно до індивідуальних потреб	*Здобувачі освіти*: індивідуальний освітній процес, який підтримує належний рівень викликів. *Педагоги* отримують переваги від детальної аналітики даних про прогрес здобувачів освіти, заощаджуючи час на планування уроків
3.	Knewton (now part of Wiley)	Технологія адаптивного навчання Knewton персоналізує подачу контенту з таких предметів, як математика та природничі науки, аналізуючи сильні та слабкі сторони кожного здобувача освіти, щоб адаптувати освітню програму в режимі реального часу	*Здобувачі освіти*: більш цілеспрямований підхід до навчання, допомога у заповненні прогалин у знаннях. *Педагоги*: рекомендації на основі ШІ скорочують час, витрачений на створення індивідуальних планів навчання
4.	Coursera	Coursera використовує машинне навчання, щоб рекомендувати здобувачам освіти персоналізовані курси та освітні матеріали на основі їх історії навчання та поведінки на платформі	*Здобувачі освіти*: отримують індивідуальні рекомендації щодо курсу та ресурси, що сприяє кращим результатам курсу. *Педагоги*: автоматизовані інструменти оцінювання та аналітика курсу зменшують адміністративні завдання

Продовження таблиці 7.1.

№ з/п	Практичний приклад	Успішне впровадження штучного інтелекту компанією в диференційоване навчання	Вплив на здобувачів освіти і викладачів
5.	Squirrel AI Learning	Китайська платформа Squirrel AI Learning використовує адаптивне навчання на основі штучного інтелекту, щоб забезпечити індивідуальне навчання для здобувачів освіти з різних предметів на основі постійного оцінювання та відгуків здобувачів освіти	*Здобувачі освіти*: переваги від високоперсоналізованих шляхів навчання, що призведе до покращення академічної успішності. *Педагоги*: штучний інтелект виконує рутинні оцінки, звільняючи час для глибшого залучення здобувачів освіти
6.	Grammarly	Grammarly використовує оброблення природної мови (NLP), щоб забезпечити персоналізований зворотний зв'язок у режимі реального часу згідно з тим, як здобувач освіти пише, допомагаючи йому покращити граматику, стиль і ясність	*Здобувачі освіти* отримують миттєвий конкретний відгук, який покращує навички письма. *Педагоги*: ШІ автоматизує процес зворотного зв'язку для написання завдань, значно скорочуючи час виставлення оцінок.

Джерело: узагальнено авторами на основі аналізу [44].

Тематичні дослідження свідчать про те, що використання інструментів ШІ забезпечує гнучкий підхід до навчання, адаптуючи його до індивідуальних потреб кожного здобувача освіти. Одночасно такі трудомісткі процеси, як оцінювання та відстеження прогресу, були значно оптимізовані для вчителів, що дозволяє зосередитися на важливіших аспектах навчання [38, 41, 43, 44, 45]. Прикладами цього є платформи DreamBox, Knewton та Coursera, які демонструють високу ефективність адаптивного навчання в підвищенні продуктивності здобувачів освіти. Крім цього, такі інструменти, як Grammarly та Squirrel AI Learning, підкреслюють важливість зворотного зв'язку в реальному часі, що суттєво покращує індивідуальний процес навчання.

Отже, можна стверджувати, що ШІ як інструмент для реалізації *диференційованого підходу* до навчання є ключовим елементом сучасної освітньої практики. Він не лише сприяє залученню здобувачів освіти, але й підвищує продуктивність викладачів, а також покращує організаційні результати освітніх процесів для всіх зацікавлених сторін [42, 45]. Натепер ШІ як важливий фактор диференційованого навчання дає можливість більш ефективно задовольняти потреби кожного здобувача освіти.

У таблиці 7.2 підсумовано значення застосування ШІ в освіті, зокрема його роль у створенні варіативності освітніх методів, наданні своєчасного зворотного зв'язку й забезпеченні інклюзивності освітніх процесів.

Таблиця 7.2. **Переваги ШІ в диференційованому навчанні**

№ з/п	Вигода	Опис
1.	Персоналізація освіти	ШІ налаштовує навчальні шляхи, аналізуючи успішність окремих здобувачів освіти і коригуючи вміст відповідно до їхніх унікальних потреб і темпу навчання
2.	Зворотний зв'язок і оцінювання в реальному часі	ШІ забезпечує миттєвий зворотний зв'язок, дозволяючи здобувачам освіти миттєво виправляти помилки, а викладачам — змінювати інструкції на основі прогресу в реальному часі
3.	Інклюзивність і доступність	Інструменти штучного інтелекту покращують доступність, пропонуючи підтримку для здобувачів освіти з обмеженими можливостями або мовними бар'єрами, як-от перетворення мови в текст і адаптивні навчальні інтерфейси

Джерело: узагальнено авторами на основі аналізу [44].

Застосування ШІ в диференційованому навчанні має низку вагомих переваг. Щонайперше, це персоналізація навчального матеріалу, що ґрунтується на адаптації змісту до індивідуальних потреб здобувача освіти, враховуючи його успіхи та труднощі. Такий підхід підвищує ефективність навчання, оскільки ШІ здатний надавати своєчасний зворотний зв'язок, пропонуючи підтримку в момент необхідності, що сприяє кращому засвоєнню знань і навичок [46]. Крім того, технології ШІ можуть сприяти подоланню проблем, пов'язаних із різноманітністю освітніх потреб. Вони пропонують інструменти, які беруть до уваги особливі потреби здобувачів освіти включно з фізичними вадами та мовними бар'єрами. Таким чином, ШІ сприяє створенню більш інклюзивного та доступного освітнього середовища для всіх здобувачів освіти.

Проте варто зазначити, що поряд із перевагами існують і певні проблеми та виклики, які слід враховувати під час інтеграції ШІ в освітній процес. Зокрема, необхідно звернути увагу на упередженість алгоритмів, захист конфіденційності даних, а також питання технічної та фінансової доступності технологій.

У таблиці 7.3 представлено основні проблеми, що виникають у процесі впровадження ШІ в освітню сферу, які потребують подальшого дослідження та розв'язання.

Отже, під час застосування ШІ в диференційованому навчанні слід ураховувати деякі виклики та ризики. По-перше, упередженість в обчислювальних алгоритмах ШІ може сприяти збереженню наявних диспропорцій у освітньому процесі, що вимагає постійних зусиль для створення більш справедливих та нейтральних інструментів. По-друге, питання конфіденційності

Таблиця 7.3. **Ключові дилеми інтеграції штучного інтелекту в освітні процеси**

№ з/п	Проблема	Опис
1.	Зміщення в алгоритмах ШІ	Системи штучного інтелекту можуть ненавмисно посилювати упередження в освітньому контенті чи оцінюванні, що призводить до нерівних можливостей для навчання
2.	Конфіденційність і безпека даних	Занепокоєння щодо того, як дані здобувачів освіти збираються, зберігаються та використовуються, що пов'язано з можливим порушенням конфіденційності та несанкціонованим доступом до приватної інформації
3.	Технічні та фінансові бар'єри	Висока вартість інструментів штучного інтелекту та цифровий розрив значно обмежують доступ до передових технологій у навчальному процесі. Особливо це стосується регіонів із недостатнім фінансуванням, де забезпечення належної технічної інфраструктури залишається дилемою. Недоступність сучасних технологій призводить до нерівності в якості освіти, що ускладнює впровадження інноваційних підходів до навчання і, відповідно, знижує ефективність інтеграції штучного інтелекту в освітні процеси на глобальному рівні.

Джерело: [52].

та безпеки даних потребують особливої уваги, адже для захисту інформації здобувачів освіти необхідно впровадити відповідні механізми. Крім того, технічні та фінансові обмеження можуть перешкоджати впровадженню ШІ в менш забезпечених освітніх закладах, що обмежує доступ до сучасних технологій.

Для повної реалізації потенціалу ШІ в освіті необхідно зосередити зусилля на подоланні цих перешкод. Особливо важливо створити безпечне освітнє середовище та зменшити технічні й фінансові бар'єри, що дозволить зробити інноваційні технології доступними для всіх освітніх закладів незалежно від їх фінансового забезпечення.

Майбутній розвиток імплементації ШІ, зокрема в освіті, є важливим етапом, на який варто очікувати, оскільки він значно покращить процес надання освітніх послуг. З удосконаленням технологій ШІ майбутні адаптивні системи навчання перевершать поточні, що застосовуються в освітніх закладах. Завдяки цим інноваціям буде забезпечено більш ефективне та індивідуалізоване надання навчальних матеріалів, а також покращений зворотний зв'язок для здобувачів освіти. Крім того, вдосконалені алгоритми та технології оброблення природної мови, що здатні краще розуміти питання та відповідати на них, значно підвищать якість навчання.

Проте разом із технологічними досягненнями виникає гостра потреба в розробленні відповідної освітньої політики, що допоможе належним чином розв'язувати етичні проблеми, які супроводжують використання ШІ в закладах освіти. Наприклад, важливими залишаються питання захисту персональних даних здобувачів освіти, а також принципів розроблення та використання алгоритмів, що застосовуються в освітньому процесі. Водночас слід розглянути, як ці технології будуть інтегровані у викладацьку та навчальну практики та яку роль у цьому процесі відіграватимуть як викладачі, так і здобувачі освіти.

Штучний інтелект може оптимізувати навчальний процес, сприяючи індивідуалізації навчання, враховуючи рівень знань, умінь та навичок здобувачів освіти. Завдяки цьому технологічному інструменту можливо адаптувати навчальні матеріали відповідно до індивідуальних потреб кожного здобувача освіти, що підвищує ефективність засвоєння інформації. Однак, незважаючи на потенціал ШІ, виникають питання, пов'язані з його інтеграцією в освітній процес, такі як забезпечення конфіденційності даних та підготовка викладачів до використання цих технологій. Це підкреслює важливість додаткової підготовки педагогічних працівників для ефективної роботи з інноваційними технологіями, забезпечуючи при цьому якість освітнього процесу на всіх етапах його реалізації.

Отже, вкрай важливо, щоб освітяни та політики тісно співпрацювали для розроблення відповідальних та справедливих підходів до впровадження ШІ. Це дозволить забезпечити захист і здобувачів освіти, і викладачів, які користуватимуться цими інструментами.

Крім того, як зазначалося вище, використання ШІ в освітньому процесі є корисним, проте варто пам'ятати, що він не здатний повністю замінити традиційні підходи до навчання. Це означає, що будь-яке впровадження ШІ повинно бути спрямоване на доповнення та покращення викладацьких навичок, надаючи викладачам інструменти для підвищення ефективності навчання і залучення здобувачів освіти до процесу. Штучний інтелект може автоматизувати трудомісткі завдання та забезпечувати цільову підтримку, що дозволить викладачам більше уваги приділяти взаємодії зі здобувачами вищої освіти, розвитку їх критичного мислення та креативності.

Упровадження ШІ в середню освіту сприяє трансформації освітнього процесу через персоналізацію навчання, що дозволяє враховувати індивідуальні особливості здобувачів освіти. Інструменти ШІ, такі як адаптивні навчальні платформи, віртуальні асистенти та рекомендаційні системи, здатні підтримувати освітній процес на новому рівні. Персоналізовані методи допомагають адаптувати контент і методи навчання відповідно до потреб кожного здобувача освіти, що підвищує якість навчання, сприяє посиленню мотивації та глибшому засвоєнню матеріалу (табл. 7.4).

Це особливо важливо всередній освіті, оскільки фундаментальні знання, отримані в школі, відіграють ключову роль у подальшому навчанні та професійному житті.

Таблиця 7.4. **Сучасні методи ШІ для персоналізації навчання**

Технологія	Опис	Приклад	Удосконалення освітнього процесу
Адаптивні навчальні платформи	Автоматичний аналіз успішності здобувачів освіти та адаптація матеріалу до їхніх потреб	Edmodo, Smart Sparrow	Поліпшує індивідуальний підхід, знижує рівень стресу
Рекомендаційні системи	Пропонують контент і завдання на основі аналізу поточних результатів та інтересів здобувачів освіти	Khan Academy, Coursera	Підвищує мотивацію до навчання, адаптує матеріал до рівня знань
Віртуальні асистенти та чат-боти	Забезпечують миттєві відповіді на запитання, допомагають у розв'язанні проблем	IBM Watson, ChatGPT	Покращують доступність знань, забезпечують підтримку
Когнітивні комп'ютерні системи	Аналізують великі обсяги даних для виявлення закономірностей у навчанні, адаптують стратегії навчання	Cognii, Kidaptive	Адаптують програми навчання на основі прогресу здобувачів
Системи аналізу емоційного стану	Відстежують емоційний стан здобувачів освіти для коригування освітнього процесу	Affectiva, Emotion AI	Підтримують емоційне благополуччя, коригують складність завдань
Гейміфікація за допомогою ШІ	Інтегрують ігрові елементи для підвищення зацікавленості та мотивації	Kahoot, Classcraft	Підвищує зацікавленість та залученість у процесі навчання
Системи автоматичної оцінки знань	Автоматизують перевірку завдань та оцінювання результатів	GradeScope, Google Forms	Прискорює процес зворотного зв'язку, підвищує об'єктивність
Платформи для співпраці на базі ШІ	Допомагають здобувачам освіти працювати в команді, аналізуючи стиль роботи кожного учасника	Microsoft Teams, Slack	Розвивають навички співпраці, підвищують ефективність командної роботи

Джерело: сформовано авторами на підставі [47, 48, 49, 52]

Сучасні технології ШІ, які інтегруються в *середню освіту*, пропонують новий підхід до навчання, кардинально відмінний від традиційного. Наприклад, адаптивні навчальні платформи, такі як Edmodo, надають можливість налаштовувати завдання індивідуально для кожного здобувача освіти. Це

суттєво відрізняється від стандартних занять, де всі здобувачі отримують однаковий матеріал незалежно від їхніх індивідуальних потреб [50]. Унаслідок використання цих платформ підвищується ефективність навчання, оскільки кожен здобувач освіти може працювати у своєму темпі, а матеріал адаптується до його рівня знань.

Рекомендаційні системи, такі як Khan Academy, дають можливість запропонувати контент і завдання відповідно до результатів, які демонструє здобувач освіти. Це відрізняється від традиційного підходу, коли здобувачі часто отримують однакові матеріали, незалежно від рівня їхньої підготовки. Таким чином, використання ШІ дозволяє зробити процес навчання динамічнішим, підвищуючи зацікавленість та мотивацію здобувачів.

Віртуальні асистенти та чат-боти, наприклад IBM Watson, забезпечують швидкий доступ до відповідей і допомоги. Традиційно здобувачі змушені чекати відповіді від викладача або шукати пояснення самостійно, що може забирати чимало часу. Застосування віртуальних асистентів дає можливість отримувати негайну допомогу, що робить навчання більш інтерактивним і доступним.

На противагу стандартним заняттям, де увага до емоційного стану здобувача освіти часто обмежена, системи аналізу емоційного стану здатні визначати, коли здобувач відчуває труднощі або втому. Це дозволяє коригувати освітнє навантаження, забезпечуючи комфортний ритм навчання та підтримуючи мотивацію.

Інтеграція інтелектуальних платформ у середню освіту створює можливість формувати динамічний "портрет" кожного здобувача освіти, дозволяючи краще розуміти його сильні сторони, прогалини в знаннях, стилі навчання та інтереси [51]. Такий "портрет" постійно оновлюється на основі даних про навчальну діяльність здобувача, включаючи час, витрачений на завдання, правильні та помилкові відповіді, темпи засвоєння матеріалу та навіть рівень мотивації. Ця інформація використовується для автоматичної адаптації освітнього процесу, завдяки чому здобувач освіти отримує завдання та ресурси, які найкраще відповідають його потребам.

Система працює циклічно, збираючи та аналізуючи нові дані для постійного вдосконалення індивідуальної траєкторії навчання. Наприклад, якщо здобувач показує швидкий прогрес у математиці, платформа може надати йому складніші завдання, які відповідають його рівню та стимулюють подальший розвиток. Навпаки, якщо здобувач стикається з труднощами в певній темі, система пропонує додаткові матеріали та вправи для кращого розуміння. Завдяки цьому платформа адаптує навчальний маршрут для кожного, надаючи можливість ефективно просуватися у власному темпі (рис. 7.1).

На *першому етапі* інтелектуальна платформа збирає різноманітні дані про навчальну діяльність здобувача освіти, включаючи час, витрачений на завдання, правильні й помилкові відповіді та інші показники. Ця інформація створює основу для подальшої індивідуалізації навчання, дозволяючи платформі формувати початковий "портрет" здобувача.

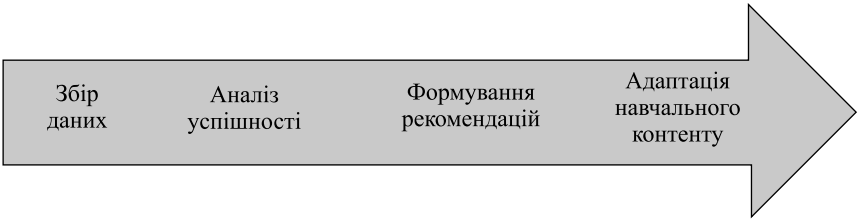


Рис. 7.1. Цикл інтеграції інтелектуальних платформ для персоналізації навчання

Далі відбувається аналіз успішності, під час якого платформа використовує зібрані дані для оцінювання рівня знань, виявлення прогалин і визначення сильних сторін здобувача освіти. Цей етап допомагає зрозуміти, які теми потребують повторення або поглиблення, що дозволяє платформі налаштовувати навчання точніше.

На основі аналізу система переходить до формування рекомендацій: здобувачеві освіти пропонуються завдання або додаткові матеріали, які відповідають його рівню підготовки. Наприклад, платформа може запропонувати додаткові вправи на повторення тем, які викликали труднощі, або надіслати більш складні завдання тим, хто вже добре опанував матеріал.

Фінальний етап — адаптація навчального контенту. Платформа коригує матеріали та завдання відповідно до індивідуальних рекомендацій, створюючи динамічний, персоналізований навчальний маршрут.

З метою визначення ефективності персоналізованих освітніх технологій у підвищенні успішності здобувачів середньої освіти під час засвоєння базових знань та формування ключових компетенцій нами здійснено опитування. Опитування здійснюється через Google Forms для забезпечення анонімності та зручності, що дозволяє респондентам відповідати в комфортний для них час і гарантує збереження конфіденційності відповідей. Респондентами виступають здобувачі середньої освіти віком 13—17 років, що навчаються з використанням персоналізованих освітніх платформ, а також Вчителі, які застосовують такі технології у своїй роботі. Залучено 150 здобувачів освіти та 50 учителів із п’яти шкіл, що вже мають досвід використання персоналізованих технологій в освітньому процесі. Така вибірка дозволяє отримати об’єктивну й комплексну оцінку, а також зіставити думки здобувачів освіти та вчителів щодо результативності даних інструментів.

Питання спрямовані на виявлення таких аспектів, як покращення рівня знань із ключових дисциплін, підвищення зацікавленості в навчанні, рівень самостійності здобувачів освіти та їхні оцінки власної здатності до критичного мислення. Питання мають як закритий формат із вибором варіантів, так і відкритий — для отримання детальнішої інформації про досвід користування персоналізованими технологіями в навчанні. Результати опитування наведено в таблиці 5, де відображено відповіді здобувачів освіти та вчителів

Таблиця 7.5. **Результати опитування щодо ефективності персоналізованих освітніх технологій у підвищенні успішності здобувачів середньої освіти**

Показник	Здобувачі освіти, які зазначили позитивний вплив (%)	Учителі, які зазначили позитивний вплив (%)
Покращення рівня знань	85	92
Підвищення мотивації до навчання	78	80
Збільшення впевненості у своїх силах	74	76
Розвиток самостійності	81	83
Підвищення здатності до критичного мислення	70	72

Джерело: [52]

за основними показниками впливу персоналізованих технологій на успішність навчання.

Очікується, що результати допоможуть оцінити, як використання індивідуально налаштованих технологій впливає на рівень знань, мотивацію до навчання та впевненість здобувачів у своїх силах.

Результати опитування вказують на суттєвий позитивний вплив персоналізованих освітніх технологій на успішність здобувачів середньої освіти. Встановлено, що 85% здобувачів освіти та 92% вчителів зазначили покращення рівня знань у ключових дисциплінах завдяки індивідуально налаштованим освітнім траєкторіям, які дозволяють адаптувати темп і складність завдань відповідно до потреб здобувача. У відкритих відповідях здобувачі освіти наголосили на можливості працювати з комфортною для них швидкістю, що знижує рівень стресу й дозволяє зосередитися на глибшому розумінні матеріалу. Це підкріплюється також відповідями вчителів, які вказали, що платформи допомагають їм легше ідентифікувати потреби здобувачів і забезпечувати їх належними ресурсами.

Важливим також є встановлене посилення мотивації до навчання: 78% здобувачів і 80% вчителів зазначили, що персоналізований підхід стимулює інтерес до освітнього процесу. У відкритих відповідях здобувачі освіти часто наголошували на мотивації, яку забезпечує можливість відстежувати свій прогрес у реальному часі. Це, як зазначали здобувачі, підвищує зацікавленість у навчанні, дозволяє отримувати негайний зворотний зв'язок і робить процес навчання більш контрольованим та особисто значущим.

Ще одним результатом є зростання впевненості у власних силах, про що повідомили 74% здобувачів освіти та 76% вчителів. Здобувачі освіти у відкритих відповідях часто описували досвід навчання як "менш стресовий", оскільки персоналізовані платформи дозволяють їм вивчати матеріал у влас-

ному темпі, без тиску, що позитивно позначається на їхньому самопочутті та здатності зосереджуватись на навчанні. Учителі підтвердили, що завдяки персоналізації здобувачі менше відволікаються, відчуваючи більшу впевненість у власних знаннях і можливостях.

Завдяки персоналізованим технологіям також покращилися навички самостійної роботи й самоконтролю, що підтвердили 81% здобувачів і 83% вчителів. У відкритих відповідях здобувачі освіти зазначили, що такі платформи допомагають їм краще планувати свій час і контролювати власний прогрес, що сприяє розвитку навичок самоорганізації. Здобувачі зазначили, що постійний зворотний зв'язок дає їм змогу швидко виправляти помилки та вдосконалювати свої знання, не чекаючи сторонньої допомоги.

Попри значні переваги, впровадження ШІ в середню освіту зумовлює появу низки викликів [53], що потребують уваги для забезпечення його ефективного й безпечного використання.

Одним із ключових викликів є можливість зниження навичок самостійності й критичного мислення в здобувачів освіти. Застосування адаптивних платформ, які автоматично пропонують завдання та матеріали на основі поточних показників, може призвести до того, що здобувачі освіти стануть менш схильними до самостійного пошуку рішень і розробки власних стратегій навчання. У надмірно автоматизованому середовищі існує ризик, що здобувачі будуть частіше покладатися на алгоритми та рекомендації систем, ніж на власні знання й навички аналізу, що в довгостроковій перспективі може уповільнити розвиток їхніх навичок самоконтролю та прийняття рішень.

Ще одним серйозним ризиком є обмеження доступу до нестандартних або більш складних завдань. Адаптивні системи, як правило, базуються на поточних рівнях знань здобувачів і коригують освітні траєкторії залежно від успішності. Проте цей підхід може мати небажаний побічний ефект: здобувачі, які швидко опановують програму, можуть залишитися в межах заданого рівня, не маючи доступу до матеріалів, що стимулюють розвиток вищих когнітивних навичок. Це може гальмувати розвиток більш обдарованих здобувачів і обмежувати їхній потенціал, оскільки система не завжди враховує індивідуальні амбіції.

Важливим викликом є також конфіденційність і безпека даних. Персоналізовані освітні платформи часто збирають великий обсяг особистих даних про кожного здобувача, включаючи інформацію про поведінку, рівень знань та прогрес у навчанні. Це створює ризик неправомірного доступу до приватних даних або неналежного їх використання. Зокрема, порушення безпеки даних може призвести до серйозних наслідків для здобувачів освіти, якщо інформація стане доступною третім сторонам. Для ефективного впровадження ШІ в освіту важливо забезпечити надійний захист даних, розробивши політику збереження конфіденційності та використання інформації лише в освітніх цілях.

Існують також технічні виклики, пов'язані з адаптацією та інтеграцією нових технологій у шкільне середовище [49]. Учителі можуть відчувати

труднощі в опануванні нових інструментів та використанні їх на практиці, що вимагає додаткових ресурсів, навчання та підтримки. Якщо вчителі не мають достатньої підготовки або технічних знань, це може призвести до неефективного використання персоналізованих платформ або ж навіть до уникання використання нових технологій, що уповільнює процес адаптації ШІ в освітньому середовищі.

Крім того, залежність від технологій в освітньому процесі може викликати проблеми у випадку технічних збоїв або недостатньої підтримки інфраструктури [54]. В умовах, коли значна частина навчання покладається на ШІ-платформи, навіть короткочасний збій може суттєво порушити освітній процес і створити додатковий стрес для здобувачів освіти та вчителів. Недостатність належної технічної підтримки або застаріле обладнання можуть зробити використання таких технологій недоступним для певних освітніх закладів, що призводить до нерівності в освітніх можливостях.

Подальше впровадження ШІ в середню освіту потребує комплексного підходу, орієнтованого на підвищення якості освітнього процесу та забезпечення відповідності вимогам сучасного суспільства [55, 56]. Проте для ефективної реалізації ШІ в шкільній системі важливо врахувати низку рекомендацій, які сприятимуть підвищенню результативності застосування цих технологій, забезпеченню безпеки даних і підтримці вчителів у процесі адаптації до нових інструментів (табл. 7.6).

Посилення безпеки даних має на меті захистити особисту інформацію здобувачів освіти від несанкціонованого доступу, що сприятиме формуванню довіри до використання нових технологій. Ця політика стане основою для прозорого застосування ШІ, забезпечуючи його використання виключно з освітньою метою. Наступною ключовою рекомендацією є підготовка вчителів, яка дозволить їм ефективно інтегрувати ШІ в освітній процес. За допомогою навчальних програм і тренінгів учителі опанують необхідні навички для роботи з адаптивними платформами, що забезпечить гнучке й продуктивне навчання.

Для підвищення рівня персоналізації важливо створити адаптивні платформи з можливістю розширених налаштувань, які дозволять здобувачам освіти працювати в зручному для них темпі. Це сприятиме формуванню комфортного освітнього середовища й підтримці індивідуального підходу, що є особливо цінним для забезпечення оптимальних умов для розвитку навичок. Окрема увага повинна бути приділена технічній підтримці інфраструктури, яка є основою для безперебійної роботи освітніх платформ на базі ШІ. Надійне забезпечення інфраструктури сприятиме зниженню ризиків технічних перешкод, що часто можуть впливати на ефективність освітнього процесу.

Нарешті, регулярний моніторинг і корекція алгоритмів ШІ є важливим аспектом, що сприяє підтримці точності рекомендацій, які платформи надають здобувачам освіти. Періодична оцінка роботи алгоритмів на основі відгуків здобувачів і вчителів дозволить оперативно вносити необхідні зміни

Таблиця 7.6. **Рекомендації щодо оптимізації процесу інтеграції ШІ в середню освіту**

Рекомендація	Пояснення	Очікуваний вплив
Забезпечення безпеки даних здобувачів освіти	Розробка політики захисту даних забезпечить контроль над інформацією про здобувачів освіти, запобігаючи ризикам несанкціонованого доступу та використання даних поза освітніми цілями	Підвищення довіри до технологій і збереження конфіденційності
Розробка навчальних програм для вчителів	Спеціальні тренінги й курси для вчителів допоможуть їм швидше опанувати нові інструменти та забезпечити ефективне впровадження ШІ в освітній процес	Підвищення ефективності використання ШІ та полегшення адаптації
Створення адаптивних платформ із розширеними налаштуваннями	Адаптивні платформи з можливістю гнучкого налаштування дозволяють кожному здобувачеві працювати у власному темпі, пропонуючи відповідні завдання та ресурси для розвитку навичок	Підвищення рівня персоналізації та гнучкості навчання
Забезпечення підтримки технічної інфраструктури	Надійна технічна підтримка та постійне оновлення обладнання гарантують безперебійну роботу платформ ШІ, знижуючи ризики від перебоїв у навчанні та втрати доступу до ресурсів	Зниження ризику технічних перешкод та підвищення стабільності процесу
Регулярний моніторинг і корекція алгоритмів ШІ	Періодичний аналіз роботи алгоритмів та їхня корекція на основі зворотного зв'язку допомагають уникати помилок і забезпечувати максимально точне налаштування освітніх траєкторій	Зменшення ризику помилкових рекомендацій та підвищення точності адаптації

Джерело: [52]

та уникати неточностей, що підвищить ефективність персоналізованого навчання й адаптивність освітнього процесу.

Таким чином, можна стверджувати, що розвиток ШІ в освітньому середовищі є перспективним для вдосконалення підходів до навчання та підвищення якості освітніх результатів. Після розв'язання етичних питань через належне регулювання політики використання штучного інтелекту в освіті ці технології зможуть стати ефективними інструментами для педагогів, що сприятиме створенню більш глибокого та результативного освітнього процесу.

Підбиваючи підсумки, можна зазначити, що штучний інтелект відіграє ключову роль у розвитку нових, більш удосконалених підходів до навчання. Він надає низку переваг, зокрема персоналізоване навчання, можли-

вість оперативного зворотного зв'язку для здобувачів освіти та сприяння інклюзивності в освітньому процесі. Штучний інтелект сприяє адаптації освітніх траєкторій до рівня знань і когнітивних особливостей здобувачів освіти, що значно підвищує ефективність засвоєння матеріалу, знижує рівень стресу та підвищує мотивацію. До того ж технології ШІ відкривають нові можливості для персоналізації освітніх програм, що дає можливість задовольнити різноманітні потреби здобувачів освіти, при цьому зменшуючи робоче навантаження на викладачів. Результати дослідження підтвердили важливість ШІ для розвитку ключових компетенцій, зокрема критичного мислення, навичок самоконтролю та здатності до аналізу.

Втім, важливо визнати наявність певних викликів, як-от алгоритмічна упередженість, питання захисту персональних даних, необхідність адаптації вчителів до нових технологій і ризики надмірної залежності здобувачів освіти від автоматизованих рішень. Крім того, існує обмеження щодо рівного доступу до технологій через недостатню технічну інфраструктуру в деяких закладах освіти, що може створювати нерівність в умовах навчання. Виявлено також, що незважаючи на високий потенціал ШІ для підвищення ефективності навчання, зберігається ризик обмеженості доступу до завдань підвищеної складності для учнів із високим рівнем знань. З огляду на виявлені проблеми рекомендується забезпечити комплексний підхід до впровадження ШІ в освіту, що включає розробку стандартів захисту даних і конфіденційності, регулярне навчання вчителів, а також створення гнучких моделей адаптації навчальних матеріалів для здобувачів із різними рівнями підготовки. Важливо також здійснювати періодичний моніторинг роботи використовуваних алгоритмів для корекції й зниження ризиків, пов'язаних із можливими помилками системи.

7.2. Штучний інтелект в науковому аналізі

Штучний інтелект, що змінив правила гри в різних галузях, вплинув і на науку. Ця трансформаційна технологія, що ґрунтується на алгоритмах машинного навчання та аналізі даних, революціонізує дослідницький ландшафт. Збір, аналіз та інтерпретація даних були трансформовані завдяки ШІ, що призвело до підвищення ефективності та результативності досліджень. Оскільки за останні роки обсяги даних зростали в геометричній прогресії, ШІ у науці дозволяє дослідникам осмислювати дедалі більші обсяги інформації, забезпечуючи розуміння, яке було б неможливим за допомогою традиційних методів [57]. Штучний інтелект приніс значні зміни в академічну сферу, революціонізувавши способи проведення досліджень, генерування знань і надання освіти. Інтеграція технологій ШІ в академічну сферу має потенціал для оптимізації процесів, покращення результатів досліджень та сприяння інноваціям.

Одним з основних способів, за допомогою якого ШІ змінює науку, є аналіз даних. Дослідники можуть використовувати алгоритми ШІ для швидкого

та ефективного аналізу величезних обсягів даних. Це дозволяє їм виявляти закономірності, кореляції та тенденції, які нелегко розпізнати традиційними методами.

Крім того, ШІ трансформує сам дослідницький процес. Він може допомогти дослідникам в огляді літератури і синтезі знань, автоматично скануючи і витягуючи релевантну інформацію з широкого спектру наукових робіт. Це не лише економить час, але й допомагає дослідникам бути в курсі останніх досягнень у своїй галузі [58].

Більше того, ШІ може розширити можливості людини в науці. Він може автоматизувати повторювані завдання, звільняючи час дослідників, щоб зосередитися на когнітивній діяльності вищого рівня. Це включає автоматизацію збору даних, аналізу і навіть написання рукописів. Оптимізувавши ці процеси, дослідники можуть приділяти більше часу критичному мисленню, генеруванню гіпотез та вивченню нових напрямків досліджень [58].

Штучний інтелект знайшов численні застосування в академічних дослідженнях у різних дисциплінах. Ось кілька прикладів того, як ШІ використовується в академічних дослідженнях [58]:

Алгоритми ШІ можуть аналізувати великі масиви даних і виявляти закономірності, кореляції та тенденції, які людині нелегко розпізнати самостійно. Це особливо корисно в таких галузях, як геноміка, кліматологія та соціальні науки.

Обробка природної мови (ОПМ): методи ОПМ дозволяють комп'ютерам розуміти і генерувати людську мову. Дослідники використовують ОПМ для аналізу великих обсягів текстових даних, вилучення інформації, узагальнення документів і виявлення настроїв. Він застосовується в таких галузях, як література, лінгвістика та соціальні науки.

Комп'ютерний зір: системи комп'ютерного зору на основі штучного інтелекту можуть обробляти та інтерпретувати візуальні дані, такі як зображення та відео. Дослідники використовують комп'ютерний зір для аналізу медичних зображень, супутникових знімків і відеозаписів з камер спостереження. Він застосовується в таких галузях, як біологія, астрономія та науки про навколишнє середовище.

Відкриття та розробка ліків: штучний інтелект використовується для прискорення процесу відкриття ліків шляхом прогнозування властивостей і взаємодії потенційних лікарських сполук. Моделі машинного навчання можуть аналізувати величезні обсяги хімічних і біологічних даних, щоб визначити потенційні мішені для ліків і розробити нові молекули.

Робототехніка та автоматизація: роботи та автоматизовані системи на основі штучного інтелекту все частіше використовуються в академічних дослідженнях для виконання таких завдань, як лабораторні експерименти, збір даних та обробка зразків. Ці роботи можуть працювати 24/7, зменшуючи кількість людських помилок і підвищуючи ефективність дослідницьких процесів.

Системи рекомендацій: алгоритми штучного інтелекту можуть надавати персоналізовані рекомендації на основі вподобань і поведінки користувача.

В академічних колах ці системи можуть пропонувати релевантні наукові статті, конференції або колаборації на основі інтересів дослідника та його попередньої роботи.

Симуляція та моделювання: методи ШІ, такі як машинне навчання та нейронні мережі, можна використовувати для створення складних моделей та симуляцій. Дослідники можуть використовувати ці моделі для вивчення та прогнозування явищ у таких галузях, як фізика, економіка та соціальні науки.

Виявлення та синтез знань: штучний інтелект може допомогти дослідникам знаходити і синтезувати інформацію з величезної кількості існуючих наукових робіт, патентів та інших академічних джерел. Це може допомогти виявити прогалини в дослідженнях, знайти релевантну літературу та згенерувати нові ідеї.

Хоча академічні дослідження з використанням ШІ мають значні переваги, існує також низка викликів та етичних міркувань, які необхідно враховувати дослідникам. Ось деякі з ключових викликів та етичних міркувань, пов'язаних із застосуванням ШІ в академічних дослідженнях [58]:

Упередженість та справедливість даних: ШІ-системи навчаються на даних, і якщо навчальні дані є упередженими або відображають суспільні упередження, моделі ШІ можуть увічнити ці упередження. Дослідники повинні ретельно відбирати і попередньо обробляти дані, щоб забезпечити справедливість і зменшити упередженість моделей ШІ.

Конфіденційність і захист даних: дослідження ШІ часто пов'язані з обробкою великих обсягів даних, зокрема персональної та конфіденційної інформації. Дослідники повинні гарантувати, що збір, зберігання та аналіз даних здійснюються з дотриманням відповідних правил конфіденційності, а також отримати інформовану згоду від учасників.

Прозорість і зрозумілість: деякі алгоритми ШІ, такі як моделі глибокого навчання, можна вважати "чорними скриньками", що ускладнює розуміння та інтерпретацію їхніх процесів прийняття рішень. В академічних дослідженнях важливо прагнути до прозорості та розробляти методи пояснення причин, що лежать в основі результатів, отриманих за допомогою штучного інтелекту.

Відтворюваність і надійність: дослідники повинні прагнути до відтворюваності, надаючи чітку документацію своїх моделей, алгоритмів і наборів даних. Важливо переконатися, що моделі ШІ є надійними і можуть добре узагальнювати невидимі дані, уникаючи надмірної підгонки або упереджених результатів.

Інтелектуальна власність та право власності: дослідження ШІ часто передбачають співпрацю та використання вже існуючих наборів даних і моделей. Необхідно встановити чіткі правила щодо прав інтелектуальної власності, володіння даними та обміну моделями і кодом ШІ між дослідниками.

Підзвітність і відповідальність: у міру того, як ШІ стає більш автономним, виникають питання підзвітності та відповідальності. Дослідники

повинні враховувати етичні наслідки своїх систем ШІ та усвідомлювати потенційні ризики і наслідки, пов'язані з їх розгортанням.

Соціальний вплив та втрата робочих місць: технології штучного інтелекту мають потенціал для революційних змін у промисловості та автоматизації певних робочих місць. Дослідники повинні пам'ятати про соціальний вплив їхніх досліджень на основі ШІ і працювати над забезпеченням справедливого переходу, створенням робочих місць і мінімізацією негативних наслідків.

Подвійне використання та зловживання: технології ШІ, розроблені для академічних досліджень, можуть мати як позитивне, так і негативне застосування. Дослідники повинні пам'ятати про потенційні сценарії подвійного використання і враховувати етичні наслідки своєї роботи, щоб запобігти зловживанням або ненавмисній шкоді.

Отже, метою наукових досліджень є розвиток суспільства завдяки поширенню знань через розроблення наукових теорій, концепцій та ідей. Науковий процес має багато етапів — від створення гіпотези, планування експерименту, моніторингу та моделювання і до публікації основних результатів. Очікується, що ШІ буде сприяти кожному етапу розвитку науки, тому використання ШІ в організації наукових досліджень має високу актуальність. Ця сучасна технологія відкриває нові можливості для підвищення ефективності наукових досліджень, проте водночас існують серйозні виклики й загрози, які слід брати до уваги, використовуючи технології ШІ на різних етапах наукових досліджень [59].

Штучний інтелект знайшов широке коло застосувань у наукових дослідженнях у різних дисциплінах. Найтиповіші випадки використання ШІ в науці сьогодення охоплюють генерування ідей, аналіз даних та розпізнавання образів, структурування тексту наукових праць, симуляцію та моделювання, виявлення та синтез знань із величезної кількості наявних наукових робіт, використання роботів та автоматизованих системи на основі ШІ для проведення експериментів [60].

Генерування ідей. У сфері наукових досліджень, яка є досить динамічною, інтеграція ШІ надає змогу значно полегшити процес генерування ідей і поліпшити дизайн досліджень [61]. На початковому етапі досліджень, а саме під час генерування ідей, алгоритми ШІ значно збагачують процеси мозкового штурму, надаючи інформацію, отриману з поточних тенденцій, історичних даних та міждисциплінарних досліджень. Застосування ШІ під час мозкового штурму прискорює процес генерування ідей, підвищує креативність людини та позитивно впливає на якість результатів. Такий підхід допомагає розвинути наявні думки та подолати творчі блоки.

Штучний інтелект і науковець мають працювати в парі, щоб ефективно здійснювати мозковий штурм, оскільки людське судження, розуміння контексту та етичні міркування відіграють вирішальну роль у вдосконаленні та реалізації ідей. Здебільшого мозковий штурм зі ШІ передбачає послідовне проходження наступних кроків. Відправна точка процесу — введення запиту

чи підказки в систему ШІ. Остання, найчастіше заснована на NLP чи алгоритмах машинного навчання, обробляє введені дані та аналізує зв'язки та закономірності в тих даних, на яких вона була навчена. Цей аналіз стає базою для генерування креативних ідей або рішень, пов'язаних із уведеними запитами. Здобуті результати підлягають детальному аналізу і опрацюванню з боку науковця з метою виокремлення корисних ідей. Найчастіше доводиться пройти кілька ітерацій із внесенням змін у запити для генерування більшої кількості результатів доти, доки не буде отримано оптимального набору ідей. На цьому етапі максимально корисним буде використання різних типів діаграм і візуальних рамок на основі текстових підказок, із подальшим упорядкуванням та категоризацією елементів на діаграмі для виявлення закономірностей, тенденцій і взаємозв'язків.

Пошук та систематизація наукових джерел. Ручне проведення систематичного огляду літератури забирає значний час та вимагає великих зусиль, потребуючи планування стратегії, проведення пошуку та аналізу літератури, систематизації здобутих результатів. Залежно від сфери дослідження кількість статей, які підлягають аналізу, може обчислюватися сотнями або тисячами, а статистика доводить, що у світі кожні 30 с публікується одна наукова стаття. Це означає, що пошук, фільтрація і вилучення ключової інформації стає дуже часозатратним процесом. З огляду на ці проблеми у сфері пошуку та огляду літератури впровадження штучний інтелект має великий вплив, підвищуючи ефективність та глибину академічних досліджень. Він полегшує вилучення та аналіз інформації з наявної літератури, синтезуючи ці висновки в послідовні огляди. Ця роль є неоціненою, оскільки інструменти ШІ обробляють та аналізують великі обсяги даних, допомагаючи створювати детальні та актуальні огляди літератури [62].

Алгоритми, що лежать в основі інструментів ШІ, зазвичай виконують дві функції — вони витягують науковий контент, забезпечують його фільтрацію, ранжування та групування результатів пошуку. Алгоритми, що витягують науковий контент, часто використовують методи NLP, які прагнуть інтерпретувати мову так, як її використовують люди. Розробники можуть, наприклад, застосовувати контрольоване машинне навчання, яке передбачає "позначення" сутностей, таких як автори статті та посилання, у навчальних наборах, щоб навчити алгоритми їх ідентифікувати та витягувати [63]. Більш складні алгоритми часто будують "графи знань", котрі деталізують зв'язки між вилученими сутностями та показують їх користувачам.

Серед інструментарів на базі ШІ, які допомагають дослідникам проводити пошук, аналіз та узагальнення наукових робіт, слід виокремити такі:

• *Genei* — дослідницький інструмент на базі ШІ, який ґрунтується на останніх досягненнях у технології NLP, вилучаючи та розбиваючи складні документи на легкозасвоювані резюме, що дає змогу користувачам швидко зрозуміти ключові моменти тексту або оптимізувати вміст своїх статей. Також доступна функція аналізу кількох документів, вбудованого керування цитуваннями та генератор посилань.

• *Consensus AI* — це пошукова система на базі ШІ. Цей інструмент надає можливість науковцям виділяти висновки з наукових статей, упорядковуючи отриману інформацію в формат резюме та надає пов'язані статті та дослідження для подальшого вивчення.

• *Scite AI* — це потужний дослідницький інструмент, який використовує ШІ, щоб надати можливість дослідникам знаходити, розуміти та оцінювати наукові статті. Scite AI класифікує цитати за трьома градаціями: допоміжні, згадувальні та контрастні, що допомагає досліднику швидко оцінити надійність і релевантність дослідження у своїй галузі. Крім цього, даний інструмент надає доступ до повних текстів статей та можливість ідентифікації суперечливих доказів.

• *Iris AI* — це платформа на основі ШІ, яка спеціалізується на наукових дослідженнях і дає змогу науковцям швидко й ефективно опрацьовувати величезні обсяги інформації. Для цього Iris AI пропонує широкий спектр інтелектуальних фільтрів, які можна налаштувати відповідно до конкретних потреб, що робить процес пошуку більш цілеспрямованим і ефективним. Як і перелічені раніше рішення, Iris AI надає можливість отримання упорядкованої інформації в форматі резюме.

• *Semantic Scholar* — безкоштовний інструмент, який використовує ШІ і методи машинного навчання, щоб аналізувати та отримувати значущі ідеї з наукових статей. Він надає графік цитувань, який дає змогу науковцям легко орієнтуватися та відшукувати дійсно авторитетні дослідження. Semantic Scholar генерує надкороткі висновки основних результатів наукової статті, допомагаючи дослідникам швидко зрозуміти, які статті додати до свого списку для читання.

*Написання та структурування тексту***.** Ще однією ключовою складовою наукових досліджень є написання та структурування тексту наукових робіт, систематизація здобутих наукових результатів та їх публікація. ШІ ефективно застосовується для підвищенні якості та змістовності дослідницького контенту, він може допомогти окреслити документ, забезпечивши логічний потік викладених результатів і їх зв'язність. Програмне забезпечення на основі ШІ, наприклад, ChatGPT чи Grammarly, Paperpal (орієнтований на англомовний текст) можуть бути корисними на етапі перевірки написаного тексту, сприяючи знаходженню та виправленню граматичних помилок та покращенню стилю письма загалом. Ці інструменти допомагають пропрацювати текст, зробити рукопис більш структурованим та лаконічним, що є критично важливим для ефективного передавання складних наукових ідей.

Штучний інтелект може допомогти інтегрувати графіку, таблиці, діаграми в дослідницький контент, тим самим значно підвищуючи його візуальну привабливість і зрозумілість. Такий підхід подання інформації дозволяє зробити складну інформацію, викладену в науковій праці, більш доступною для ширшої аудиторії. Прикладом інноваційних систем з інтегрованим ШІ, які використовують машинне навчання для створення зображень із тексту, є DALL-E 2, Canva AI Art Generator.

Перевірка наукових тверджень. Між етапом формування мети дослідження та отриманням наукових результатів може пройти тривалий та трудомісткий процес теорії, експериментів, перевірки та повторення. На етапі перевірки наукових тверджень використовують методи машинного навчання і оброблення природної мови, що значною мірою підвищує якість цього етапу та зменшує витрати часу на його реалізацію.

Застереження щодо використання ШІ в наукових дослідженнях. Наукові дослідження та етика публікацій мають вирішальне значення для підтримання цілісності та довіри до наукової громади. Раніше було розглянуто переваги, які надає використання ШІ під час проведення наукових досліджень. Однак було б помилкою водночас з перевагами не розглянути слабкі сторони дослідницьких інструментів на основі ШІ та потенційну небезпеку їх активної інтеграції в наукову діяльність. Надлишкове використання ШІ може призвести до створення шахрайських наукових робіт. З огляду на це, постає потреба в пильності щодо підтримання академічної доброчесності. Академічна доброчесність — це моральний кодекс та етична політика наукової роботи, яка має важливе значення в спільноті науковців.

Застереження, щодо використанні ШІ під час наукових досліджень:

враховуйте недосконалість інструментів ШІ і перевіряйте вихідні дані інструментів ШІ та їхню точність;

не слід забувати, що використання ШІ для генерування ідей під час написання наукової роботи також має бути відображено в посиланнях;

не слід використовувати ШІ як основу наукового дослідження, а тільки як доповнення до власних досліджень і тверджень;

ШІ працює на основі алгоритмів та великої кількості даних, які він вивчив. Хоча він може створювати нові комбінації ідей, вони все одно базуються на тому, що він вже знає. Саме тому, не слід намагатися отримати наукову новизну в написаних ШІ роботах.

Використання програм, які функціонують на базі технологій ШІ, здатні значно підвищити рівень продуктивності під час проведення наукових досліджень. Основні етапи наукового дослідження, коли ШІ може покращити академічні функції, узагальнено в таблиці 7.7.

Отже як показують дослідження, інтеграція ШІ в наукові дослідження має потенціал на кожному етапі наукового процесу: від генерування гіпотез і побудови математичних доказів до планування експерименту та моніторингу, збору та аналізу даних, моделювання та швидкого висновку. Використання штучного інтелекту в науковій сфері можливе в разі дотримання певних правил, пов'язаних із конфіденційністю даних, етичністю, академічною доброчесністю та відповідальністю використання інформації штучного інтелекту.

Отже, використання штучного інтелекту сьогодні революціонізує наукові дослідження [57]. У різних галузях науки штучний інтелект використовується для аналізу величезних обсягів даних, автоматизації рутинних завдань

Таблиця 7.7. **Основні етапи наукового дослідження, коли штучний інтелект може покращити академічні функції**

Етапи наукового дослідження	Можливості штучного інтелекту для покращення наукової діяльності
Генерація ідеї дослідження	1. Алгоритми ШІ значно збагачують процеси мозкового штурму, виявляють прогалини у наявних дослідженнях, генерують гіпотези. 2. Алгоритми ШІ допомагають у розробленні основних етапів дослідження
Пошук та систематизація наукових джерел	1. ШІ полегшує вилучення та аналіз інформації з наявної літератури, синтезуючи ці висновки в послідовні огляди. 2. Фільтрація, ранжування та групування результатів пошуку. 3. Упорядкування отриманої інформації у формат резюме. 4. Формування списку пов'язаних статей та досліджень для подальшого вивчення
Генерування тексту	1. ШІ може допомогти в написанні тексту, а саме в розширенні тексту, автозаповненні. 2. Надає можливість автоматизувати написання певних розділів статті, зокрема вступу або переліку посилань
Узагальнення тексту	Моделі ШІ можна використовувати для узагальнення наукових дослідницьких робіт, що полегшує роботу дослідників і надає можливість швидко зрозуміти ключові висновки статті
Структурування тексту	1. ШІ може допомогти окреслити документ, забезпечивши логічний потік викладених результатів. 2. ШІ може допомогти інтегрувати графіку, таблиці, діаграми в дослідницький контент, тим самим значно підвищивши його візуальну привабливість і зрозумілість
Перевірка граматики та мови	Моделі ШІ можна використовувати для перевірки граматичних та мовних помилок у науковій роботі

Джерело: [59].

і нових відкриттів, які ще кілька років тому було неможливо уявити. Перевірте, що вже відкрито в деяких галузях науки.

Фармакологія

Завдяки розвитку штучного інтелекту в науці були відкриті нові ліки, можна зрозуміти хвороби, а складні молекулярні дані продовжують вивчатися. Генетичні дані обробляються алгоритмами штучного інтелекту, щоб зрозуміти першопричину таких захворювань, як рак, і розробити ефективні методи лікування.

Нові відкриття показують, що штучний інтелект може бути використаний у розробці ліків як засіб прогнозування потенційних властивостей ліків, допомагаючи оптимізувати процес розробки ліків в цілому.

Фізика та астрономія

Використання штучного інтелекту у фізиці дозволило зробити нові відкриття про фундаментальну природу Всесвіту, аналізуючи дані, зібрані за допомогою прискорювачів частинок, телескопів та інших інструментів. Вчені також використовують алгоритми штучного інтелекту для моделювання поведінки складних дисциплінарних систем, що дозволяє їм перевіряти свої теорії і краще розуміти навколишній світ.

Космічний телескоп "Габбл" та інші супутникові місії використовують ШІ для аналізу величезних обсягів даних з телескопів. Небесні об'єкти, такі як зірки, галактики і чорні діри, ідентифікуються і класифікуються за допомогою алгоритмів штучного інтелекту, а їхні властивості і поведінка також вивчаються за допомогою цих алгоритмів.

Хімія

Існує також багато застосувань штучного інтелекту в хімії, наприклад, аналіз великих масивів даних, автоматизація рутинних завдань і розробка нових сполук на основі використання штучного інтелекту. Люди все частіше використовують алгоритми штучного інтелекту для прогнозування властивостей потенційних нових матеріалів, таких як надпровідники, а також для розробки каталізаторів, які можуть бути використані для підготовки хімічних речовин до використання в хімічних реакціях.

Наука стрімко трансформується завдяки штучному інтелекту. Штучний інтелект допомагає вченим відкривати нові речі та поглиблювати наше розуміння світу, спрощуючи процеси та полегшуючи аналіз даних.

Майбутнє ШІ в академічних дослідженнях має величезний потенціал для трансформаційних досягнень. Ось деякі тенденції, можливості та потенційні наслідки, на які варто звернути увагу [58].

Міждисциплінарна співпраця: штучний інтелект об'єднує дослідників з різних дисциплін, сприяючи співпраці та уможливлюючи проривні ідеї.

Відкриття на основі даних: Алгоритми штучного інтелекту витягують цінну інформацію з великих масивів даних, революціонізуючи дослідження в різних галузях.

Персоналізоване та адаптивне навчання: Технології штучного інтелекту забезпечують індивідуальний освітній досвід, оцінюючи успішність учнів і пропонуючи цільовий зворотний зв'язок.

Посилення наукових відкриттів: Штучний інтелект допомагає дослідникам генерувати гіпотези, планувати експерименти та аналізувати дані, прискорюючи дослідницький процес.

Етичні міркування та відповідальний ШІ: Дослідники розглядають питання упередженості, прозорості, конфіденційності та підзвітності, щоб забезпечити етичне та відповідальне використання ШІ.

Автоматизація з використанням штучного інтелекту: Штучний інтелект впорядковує дослідницькі робочі процеси, автоматизуючи такі завдання, як збір та аналіз даних, підвищуючи ефективність.

AI для глобальних викликів: Штучний інтелект сприяє вирішенню проблем зміни клімату, охорони здоров'я та бідності, аналізуючи дані та оптимізуючи розподіл ресурсів.

Підвищена креативність: Штучний інтелект виступає в ролі творчого партнера, генеруючи ідеї, синтезуючи інформацію та розширюючи межі в таких сферах, як мистецтво та дизайн.

Покращена експертна оцінка та наукова комунікація: Штучний інтелект автоматизує деякі аспекти експертного оцінювання, допомагає в перекладі та рекомендує релевантні наукові статті.

Демократизація досліджень: Платформи штучного інтелекту надають доступ до обчислювальних потужностей, наборів даних і можливостей співпраці в усьому світі, демократизуючи дослідження.

Як ШІ змінить ситуацію в науці? З'являться нові відкриття, а складні проблеми вирішуватимуться ефективніше і швидше. Ще однією перевагою ШІ є його здатність долати деякі обмеження традиційних методів дослідження, такі як складність моделювання складних систем і доступ до великих масивів даних. Технологія дозволить дослідникам отримувати результати в режимі реального часу з різних джерел і виявляти закономірності, які раніше було неможливо виявити.

Застосування ШІ в науці має потенціал революціонізувати науку і матиме значний вплив на наше розуміння світу. Ключ до забезпечення етичного та відповідального використання штучного інтелекту в науці полягає в тому, щоб його переваги розподілялися порівну між усіма. Відповідальне використання штучного інтелекту визначатиме майбутнє науки, і ми повинні переконатися, що він використовується для загального блага.

Інструменти штучного інтелекту, які застосовують в академічних дослідженнях [58].

Картинка: Pictory — це відеогенератор на основі штучного інтелекту, який спрощує процес створення та редагування високоякісних відео.

Джаспер.: Jasper є найкращим помічником для написання текстів зі штучним інтелектом, який встановлює стандарти на ринку завдяки своїм винятковим функціям і чудовій якості.

Мерф.: Murf, генератор тексту в мовлення, широко визнаний як один з найпопулярніших і найвидатніших ШІ-генераторів голосу, доступних на ринку.

HitPaw Photo Enhancer: інструмент на основі штучного інтелекту для покращення якості та деталізації зображень.

ChatGPT: ШІ-модель для обробки природної мови та генерування текстових відповідей, схожих на людські.

Lovo.ai: Lovo.ai отримав нагороди як генератор голосу та рішення для перетворення тексту в мовлення.

Reply.io: Reply пропонує комплексну платформу для залучення продажів, яка дозволяє масштабувати створення нових можливостей, забезпечуючи при цьому персоналізований підхід у кожній взаємодії.

Стратегія розвитку ШІ в Україні передбачає розвиток основних напрямів ШІ як самостійних наукових напрямів [26]:

нечіткі множини та нечітка логіка;

штучні нейронні мережі;

гібридні нейронечіткі та нечітко нейронні мережі;

біоінспіровані метаевристичні алгоритми оптимізації (еволюційні та мультиагентні алгоритми, алгоритми, що імітують фізичні та інші процеси), біоінформатика, машинне навчання і под.

Передбачено впровадження методів і технологій ШІ в інших сферах науки та освіти — зокрема, для оптимізації навчального процесу та профілювання здобувачів освіти за здібностями — а також розвиток міждисциплінарних досліджень на перетині ШІ та інших галузей науки.

Планується впровадження навчальних дисциплін, які будуть вивчати ШІ на різних етапах освіти. Буде розширено, уніфіковано і систематизовано мережу навчальних центрів, спрямованих на підготовку висококваліфікованих кадрів для України у сфері ШІ.

Планується створення трансдисциплінарних кластерів щодо забезпечення моніторингових досліджень пізнавального й інтелектуального розвитку учнів, відповідності навчальних програм та змісту навчальних і методичних матеріалів викликам наукового та науково-технічного розвитку суспільства, якості змісту викладання основ наук.

Імплементація в навчальний процес інтелектуальних платформ трансдисциплінарної освіти, як організації інтегрованого використання в освіті описів образів картини світу на принципах забезпечення операціональності досліджень здобувачам освіти навколишнього світу через функціональну взаємодію тематично різноманітних систем знань. Це забезпечить формування умов щодо змістовного наповнення освіти, як процесу прогресивних змін властивостей і якостей особистості, необхідною умовою якого є особливим чином організована її навчально-дослідницька діяльність.

Особливу увагу буде приділено розвитку базових цифрових навичок [26]:

аналіз даних із застосуванням програмного забезпечення;

навички програмування;

навички розробки, проєктування та обслуговування технологій;

знання та навички для моделювання, взаємодії та підвищення довіри до машинних агентів/роботів (комфортність співпраці “людина-машина”);

загальні навички користування сучасною персональною комп’ютерною технікою;

опрацювання та інтерпретація складної інформації;

навички вирішення проблем у вибудуваній завдяки цифровим технологіям співпраці в командах (міжкультурних або дистанційних).

Отже, штучний інтелект, безперечно, трансформує освіту, але не зможе повністю замінити собою викладача, наставника, наукового керівника тощо. Тому що навчальний процес багатогранний і не обмежується лише розв'язанням поставлених завдань. Людська взаємодія в освітньому процесі та науковому аналізі незамінна і має безліч завдань. Це, перш за все, адаптація до нового навчального середовища, становлення та розвиток емоційного інтелекту, виховна функція, мотивація, контроль, покарання та заохочення, диференціація навчання та індивідуальний підхід. Освітній процес має на меті формування гармонійної, всебічно розвиненої особистості з чіткими переконаннями та цінностями, а не просто набір певних знань, умінь та навичок для виконання завдань. Безумовно, етична взаємодія людини з технологіями ШІ може дати нові наукові прориви, разом із тим, і потенціал для зловживання цією технологією також очевидний. Штучний інтелект варто розглядати як новий інструмент, який зможе значно допомогти як у процесі здобуття знань, так і в процесі контролю якості та успішності цих знань, покращити освітні результати через трансформацію освіти та нові потужні технології [64, 65]:

Перший спосіб — зміна бізнес-моделей освітніми компаніями. Turnitin прискорив запуск детектора ШІ, Duolingo використав GPT-4, щоб допомогти учням перевірити свої мовні навички, а компанія Chegg відчула зменшення кількості підписок на свої послуги, оскільки багато потенційних клієнтів почали звертатись по допомогу до ШІ. Постраждав видавничий та освітній сектор. Компанії мають усвідомити це та проаналізувати, як змінюються вимоги студентів і працювати, щоб заповнити ці прогалини.

Другий спосіб — використання ботів для допомоги у навчанні. Ці боти можуть надати особисту підтримку, підтримку благополуччя та консультації 24/7, чого студенти раніше ніколи не могли мати.

Третій спосіб — зменшення тиску на репетиторів під час підготовки вступу до закладів вищої освіти. Використання ШІ дозволить аналізувати рівень підготовки абітурієнтів та оцінювати його щоб звільнити час персоналу для роботи з найбільш перспективними кандидатами.

Четвертий спосіб — новий стиль роботи з пошуку наукових статей і аналізу цитувань. Свого часу науковці покладались на каталог університетської бібліотеки або GoogleScholar для вивчення наукових робіт. На початку 2020-х років на ринку з'явилася низка нових інструментів (Connected Papers, Inciteful, LitMaps), кожен з яких забезпечує набагато зручнішу візуалізацію пошукових результатів. ResearchRabbit чудово підходить не лише для визначення широко цитованих статей, але й для надання корисних графіків, які показують, хто саме їх цитує. Серед нових продуктів на ринку стартап із Брукліна Scite. Він обіцяє надавати "надійні відповіді безпосередньо з повного тексту дослідницьких статей" на додаток до функціоналу визначення корисних статей, аналізу цитат і перевірки фактів за допомогою ШІ.

П'ятий спосіб — пошук текстів для читання. Менше 10-ти років тому Інститут штучного інтелекту Аллена запустив Semantic Scholar з інстру-

ментом обробки природної мови, який надає однорядкові резюме наукової літератури. Станом на минулий рік його текстовий корпус охоплює понад 200 млн публікацій у всіх галузях знань. Оновлена за допомогою ШІ версія Bing використовується для перегляду та оцінки наукових досліджень. Таким чином, вже немає необхідності опрацьовувати першоджерела щоб зрозуміти суть проблеми, предмет чи об'єкт дослідження, створені за допомогою ШІ резюме виявляються більш корисними для не фахівців, ніж авторські анотації, адже не потребують зайвих зусиль, часу та не несуть інтелектуального навантаження.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінет Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 23.03.2025).
2. Програма великої трансформації "Освіта 4.0: український світанок". URL: https://mon.gov.ua/storage/app/media/news/2022/12/10/Osvita-4.0.ukrayinskyy.svitanok.pdf (дата звернення: 23.03.2025).
3. Turing A. M. Computing Machinery and Intelligence. Mind. 1950. Vol. 49. No. 236. P. 433—460. URL: https://doi.org/10.1093/mind/LIX.236.433 (дата звернення: 23.03.2025).
4. Newell A., Shaw C., Simon H. Report on a General Problem-Solving Program. *Proceedings of the International Conference on Information Processing*. 1959. P. 256 –264.
5. McCarthy J., Minsky M.L., Rocheśter N., Shannon C.E. A proposal for the Dartmouth summer research project on Artificial Intelligence, 1955. *AI Magazine*. 2006. Vol. 27. No. 4. P. 12—14.
6. Robinson J. A machine-oriented logic based on the resolution principle. *Journal of the ACM (JACM)*. 1965. Vol. 12. No. 1. P. 23—41. URL: https://doi.org/10.1145/321250.321253 (дата звернення: 23.03.2025).
7. Weizenbaum J. ELIZA — a computer program for the śtudy of natural language communication between man and machine. In Communication of the ACM. 1966. Vol. 9. No. 1. P. 36—45. URL: https://doi.org/10.1145/365153.365168 (дата звернення: 23.03.2025).
8. Rubin P. A Conversation with Jaron Lanier, VR Juggernaut. The Wired : website. 2017. URL: https:// www.wired.com/story/jaron-lanier-vr-interview/ (дата звернення: 23.03.2025).
9. Біокібернетика Миколи Амосова. Інформаційні технології в Україні: історії та особистості: вебсайт. http://ua.uacomputing.com/stories/nikolay-amosovs-bio-cybernetics (дата звернення: 23.03.2025).
10. Hinton G., Osindero S., Teh Y. A fast learning algorithm for deep belief nets. *Neural Computation*. 2006. Vol. 18. P. 1527—1554. URL: https://doi.org/10.1162/neco.2006.18.7.1527 (дата звернення: 23.03.2025).
11. Fukuyama F. Political order and political decay : from the industrial revolution to the globalization of democracy. New York : Farrar, Strauss and Giroux, 2014. 672 p.
12. Погореленко А. Штучний інтелект : сутність, аналіз застосування, перспективи розвитку. *Економічні науки*. 2018. Вип. 32. С. 22—27.

13. Sadiku M. N., Ashaolu T. J., Ajayi-Majebi A. & Musa S. M. Artificial intelligence in education. *International Journal of Scientific Advances* (IJSCIA). 2021. Vol. 2 (1). P. 5—11. URL: https://doi.org/10.51542/ijscia.v2i1.2 (дата звернення: 23.03.2025).
14. Joshi S., Rambola R. K. & Churi P. Evaluating artificial intelligence in education for next generation. In Journal of Physics : Conference Series. Bristol: IOP Publishing. 2021. Vol. 1714 . No. 1. P. 12—39. URL: https://doi.org/10.1088/1742-6596/1714/1/012039 (дата звернення: 23.03.2025).
15. Chen L., Chen P. & Lin Z. Artificial intelligence in education : a review. Ieee Access. 2020. Vol. 8. P. 75264–75278. URL: https://doi.org/10.1109/ACCESS.2020.2988510 (дата звернення: 23.03.2025).
16. Panigrahi C. M. Use of artificial intelligence in education. Management Accountant. 2020. Vol. 55 (5). P. 64—67. URL: https://doi.org/10.33516/maj.v55i5.64-67p. (дата звернення: 23.03.2025).
17. Huang J., Saleh S. & Liu Y. A review on artificial intelligence in education. *Academic Journal of Interdisciplinary Studies*. 2021. Vol. 10 (3). P. 206—206. URL: https://doi.org/10.36941/ajis-2021-0077 (дата звернення: 23.03.2025).
18. Aleven V., Roll I., McLaren B. M. and Koedinger K. R. Help helps, but only so much : research on help seeking with intelligent tutoring systems. *International Journal of Artificial Intelligence in Education*. 2016. Vol. 26. P. 205—223. URL: https://doi.org/10.1007/s40593-015-0089-1 (дата звернення: 23.03.2025).
19. Dillenbourg P. The evolution of research on digital education. *International Journal of Artificial Intelligence in Education*. 2016. Vol. 26. P. 544—560. URL: https://doi.org/10.1007/s40593-016-0106-z (дата звернення: 23.03.2025).
20. Panukhnyk O. Artificial intelligence in the educational process and scientific research of higher education applicants: responsible boundaries of AI content. *Galician economic journal*. vol. 83, no 4, pp. 202—211. URL: https://doi.org/10.33108/galicianvisnyk_tntu2023.04.202 (дата звернення: 23.03.2025).
21. Коломієць А. М., Кушнір О. І. (2024). Використання штучного інтелекту в освітній та науковій діяльності: можливості та виклики. (2024). *Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems*, *70*, 45-57. https://doi.org/10.31652/2412-1142-2023-70-45-57 (дата звернення: 23.03.2025).
22. Назар, М. М. (2024). Штучний інтелект: на початку ери нових можливостей системи освіти: Наукова доповідь загальним зборам НАПН України "Захист і підтримка ментального здоров'я українців в умовах воєнного стану: виклики і відповіді", 22 листопада 2024 р. *Вісник Національної академії педагогічних наук України*, *6*(2), 1-4. URL: https://doi.org/10.37472/v.naes.2024.6224 (дата звернення: 23.03.2025)..
23. Поліщук О., Поліщук О., Дудченко В. Філософія штучного інтелекту в освітньому процесі. Humanities studies : Collection of Scientific Papers. 2022. Вип. 13 (90). С. 103–109. URL: https://doi.org/10.26661/hst-2022-13-90-12 (дата звернення: 23.03.2025).
24. Певень, К.О., Хміль, Н.А., & Макогончук,Н.В. (2023). Вплив штучного інтелекту на зміну традиційних моделей навчання та викладання: аналіз технологій для забезпечення ефективності індивідуальної освіти. *Перспективи та іннова-*

ції науки, 11(29). URL: https://doi.org/10.52058/2786-4952-2023-11(29)-306-316 (дата звернення: 23.03.2025).
25. Панок, В.Г., Назар, М.М., & Старков, Д.Ю. (2024). Про методологію розробки чат-бота на основі штучного інтелекту для психологічної підтримки громадян України. Віртуальний освітній простір: психологічні проблеми: XII Міжнародна науково-практична інтернет-конференція. URL : https://newlearning.org.ua/sites/default/files/tezy/2024/Panok_Nazar_Starkov_2024.pdf (дата звернення: 23.03.2025).
26. Стратегія розвитку штучного інтелекту в Україні: монографія / А.І. Шевченко, С.В. Барановський, О.В. Білокобильський та ін. [За заг. ред. А.І.Шевченка]. Київ: ІПШІ, 2023. 305 с.
27. ISO/IEC TR 24028:2020(en) Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence URL: https://www.iso.org/standard/77608.html (дата звернення: 23.03.2025).
28. Штучний інтелект. Як він вплине на освіту. URL: https://nus.org.ua/articles/shtuchnyj-intelekt-yak-vinvplyne-na-osvitu/ (дата звернення: 23.03.2025)
29. Громова, І. І., Мартинюк, Н. В., & Шевченко, О. В. (2020). Система підготовки майбутніх вчителів до використання технологій штучного інтелекту. *Інформаційні технології в освіті*. 39. С. 19—33.
30. Лисенко, О. В. (2020). Використання технологій штучного інтелекту у підготовці майбутніх учителів інформатики. *Проблеми сучасного педагогічного процесу*. Вип.1(62). С. 184—187.
31. Солодков, А. В., Полякова, Л. Ю. (2020). Технології штучного інтелекту як засіб вдосконалення підготовки майбутніх учителів інформатики. *Міжнародний науковий журнал "Інтернаука"*. Вип. (2). С. 11—16.
32. Чепіль, Т. В. Використання технологій штучного інтелекту в освітньому процесі підготовки майбутніх учителів. *Наукові записки Національного університету "Острозька академія"*. Серія "Педагогічні науки", (25). С. 128—133.
33. Жихорська, О. (2024). Використання чат-ботів у навчанні студентів. *Вісник Київського національного університету імені Тараса Шевченка. Серія «Педагогіка»*, *2*(18). URL: https://doi.org/10.17721/2415-3699.2023.18.06 (дата звернення: 23.03.2025).
34. Самчинська, Я. Б., Шерман, М. І., & Сікелінда, М. О. (2020). Імплементація теми з розробки чат-ботів в університетський курс "офісні комп'ютерні технології". Електронне наукове фахове видання "Відкрите освітнє е-середовище сучасного університету", (9), 121—133. URL: https://doi.org/10.28925/2414-0325.2020.9.10 (дата звернення: 23.03.2025).
35. Hariri, R. (2019). Artificial intelligence in education. Handbook of Research on Digital Content, Mobile Learning, and Technology Integration Models in Teacher Education. P. 1–17.
36. Lee, I., Lee, J., Lee, K., Lee, J., & Hwang, J. (2019). Effectiveness of artificial intelligence in education: *A systematic review. Journal of Educational Technology & Society*. V. 22(3), 47—63.
37. Yilmaz, R., & Karakus, T. (2020). Artificial intelligence-based educational applications: *A systematic review of the literature. Journal of Educational Technology & Society*. V. 23(3), p. 1—15.

38. Analysing the Impact of Artificial Intelligence and Computational Sciences on Student Performance: Systematic Review and Meta-analysis / I. García-Martínez et al. *Journal of New Approaches in Educational Research*. 2023. Vol. 12, no. 1. P. 171. URL: https://doi.org/10.7821/naer.2023.1.1240 (дата звернення: 17.02.2025).
39. Aktay S. The usability of images generated by artificial intelligence (AI) in education. *International Technology and Education Journal.* Vol. 6 No. 2. P. 51–62. URL: https://itejournal.com/articles/the-usability-of-images-generated-by-artificial-intelligence-ai-in-education.pdf (дата звернення: 17.02.2025).
40. Громова І. І., Мартинюк Н. В., Шевченко О. В. Система підготовки майбутніх вчителів до використання технологій штучного інтелекту. *Інформаційні технології в освіті*. 2020. № 39. С. 19—33.
41. Glazunova O., Shyshkina M. The concept, principles of design and implementation of the university cloud-based learning and research environment. *Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Volume II: Workshops*. 2018. P. 332—347. URL: http://ceur-ws.org/Vol-2104/paper_158.pdf (дата звернення: 17.02.2025).
42. Папач, О. І., Горожанкіна, О. Ю., & Різак, Г. В. (2024). Аналіз ролі штучного інтелекту у впровадженні диференційованого підходу до навчання. *Педагогічна Академія: наукові записки*, (10). URL: https://doi.org/10.5281/zenodo.13827888 (дата звернення: 17.02.2025).
43. Hariri R. Artificial intelligence in education. *Handbook of Research on Digital Content, Mobile Learning, and Technology Integration Models in Teacher Education*. 2019. P. 1–17. URL: https://www.daneshnamehicsa.ir/userfiles/files/1/17-%20Handbook%20of%20Research%20on%20Digital%20Content,%20Mobile%20Learning,%20and%20Technology%20Integration%20Models%20in%20Teacher%20Education.pdf (дата звернення: 17.02.2025).
44. Koldovskiy A. A transdisciplinary approach to improving the quality of the scientific and educational process in the context of digital transformation. *Sixth International Scientific and Practical WEB Forum on the Development of a Unified Open Information Space for Lifelong Education*, Kyiv-Kharkiv, Ukraine, 2024. URL: http://repo.uipa.edu.ua/jspui/bitstream/123456789/8103/1/ZbForumSOIS-2024-45-48.pdf. (дата звернення: 17.02.2025).
45. Moroianu N., Iacob S.-E., Constantin A. Artificial Intelligence in Education: a Systematic Review. *Geopolitical perspectives and technological challenges for sustainable growth in the 21st century*. 2023. P. 906—921. https://doi.org/10.2478/9788367405546-084 (дата звернення: 17.02.2025).
46. Cultural exchange and cross-border dynamics in Europe: exploring language, heritage, and shared ideals / O. Ardelian et al. *Multidisciplinary Science Journal*. 2024. Vol. 6. P. 2024ss0708. URL: https://doi.org/10.31893/multiscience.2024ss0708 (дата звернення: 23.02.2025).
47. Топузов О., Алексєєва С. Можливості використання штучного інтелекту в освітньому процесі закладів середньої освіти в умовах воєнного стану. *Український педагогічний журнал.* 2024. № 1. С. 5—11. URL: https://lib.iitta.gov.ua/id/eprint/740422/ (дата звернення: 25.02.2025).
48. Мар'єнко М. Добір сервісів штучного інтелекту для використання у навчанні природничо-математичних предметів у закладах загальної середньої освіти. *На-*

укові записки. Серія: Педагогічні науки. 2024. № 214. С. 256—261. URL: https://doi.org/10.36550/2415-7988-2024-1-214-256-261 (дата звернення: 23.02.2025).
49. Кочарян А., Ячменик М., Гарасимчук І. Інтеграція віртуальної реальності та штучного інтелекту в освітній процес. *Наука і техніка сьогодні.* 2024. № 1(29). С. 488—500. URL: https://doi.org/10.52058/2786-6025-2024-1(29)-488-500 (дата звернення: 23.02.2025).
50. Park J., Teo T. W., Teo A., Chang J., Huang J. S., Koo S. Integrating artificial intelligence into science lessons: teachers' experiences and views. *International Journal of STEM Education.* 2023. Vol. 10. № 61. URL: https://doi.org/10.1186/s40594-023-00454-3 (дата звернення: 23.02.2025).
51. Lytvynova S., Vodopian N., Sysoeva O. Artificial Intelligence in Secondary Education: An Innovative Teacher's Tool to Ensure Individualised Learning for Students. In: Tomczyk Ł. (eds) *New Media Pedagogy: Research Trends, Methodological Challenges, and Successful Implementations.* Springer, Cham, 2024. URL: https://doi.org/10.1007/978-3-031-63235-8_26 (дата звернення: 23.02.2025).
52. Чернова, Т. Ю., Охман, Н. І., & Бондар, Є. В. (2024). Моделі інтеграції штучного інтелекту в освітній процес для покращення індивідуального навчання здобувачів середньої освіти. URL: https://doi.org/10.5281/zenodo.14057423 (дата звернення: 23.02.2025).
53. Гайдамака І. Етичні аспекти використання штучного інтелекту в освітньому процесі закладів загальної середньої освіти. *Проблеми освіти.* 2024. № 1 (100). URL: https://imzo-journal.org.ua/index.php/journal/issue/download/19/1-2024-pdf#page=57 (дата звернення: 23.02.2025).
54. Saputra I., Astuti M., Sayuti M., Kusumastuti D. Integration of Artificial Intelligence in Education: Opportunities, Challenges, Threats and Obstacles. A Literature Review. *The Indonesian Journal of Computer Science.* 2023. Vol. 12. № 4. URL: https://doi.org/10.33022/ijcs.v12i4.3266. (дата звернення: 23.02.2025).
55. Морзе Н., Кравчук А., Бондаренко К. Якою має бути цифрова компетентність вчителів у галузі використання штучного інтелекту? *Відкрите освітнє е-середовище сучасного університету.* 2024. № 16. С. 76—91. URL: https://doi.org/10.28925/2414-0325.2024.166. (дата звернення: 23.02.2025).
56. Павліха Н., Науменко Н., Корнелюк О. Розвиток та регулювання штучного інтелекту в Україні у воєнний та повоєнний періоди: сучасні тенденції та перспективи. *Цифрова економіка та економічна безпека*. 2023. № 8(08). С. 105—111. URL: https://doi.org/10.32782/dees.8-18 (дата звернення: 23.02.2025).
57. Artificial intelligence in Science. URL : https://mindthegraph.com/blog/artificial-intelligence-in-science/ (дата звернення: 23.02.2025).
58. Exploring the role of AI in academic research. [Електронний ресурс]. URL : https://mindthegraph.com/blog/uk/ai-in-academic-research/?utm_source=chatgpt.com (дата звернення: 23.02.2025).
59. Полоневич О. В., Морозова С. В., Аверічев І. М., Полоневич А. П. Використання штучного інтелекту в організації наукових досліджень. Зв'язок. № 3 (169), 2024. 3—6. URL: https://doi.org/10.31673/2412-9070.2024.030306 (дата звернення: 23.02.2025).
60. Вивчення ролі штучного інтелекту в академічних дослідженнях. URL: https://mindthegraph.com/blog/uk/ai-in-academ-ic-research (дата звернення: 23.02.2025).

61. Alshater, Muneer, Exploring the Role of Artificial Intelligence in Enhancing Academic Perfor mance: A Case Study of ChatGPT. URL: http://dx.doi.org/10.2139/ssrn.4312358 (дата звернення: 23.02.2025).
62. Mohamed Khalifa, Mona Albadawy. Using artificial intelligence in academic writing and research: An essential productivity tool, Computer Methods and Programs in Biomedicine Update, Volume 5, 2024. URL: https://doi.org/10.1016/j.cmpbup.2024.100145 (дата звернення: 23.02.2025).
63. How AI technology can tame the scientific literature (Nature 561, 273–274; 2018). URL: https://www.nature.com/articles/d41586-018-06617-5 (дата звернення: 23.02.2025).
64. Tom, Williams, Jack, Grove Five ways AI has already changed higher education. URL: https://www.timeshighereducation.com/depth/five-ways-ai-has-already-changed-higher-education?utm_source=newsletter&utm_medium=email&utm_campaign=editorial-weekly&spMailingID=25829776&spUserID=MTAxNzcwOTEyM (дата звернення: 23.02.2025).
65. Андрощук Аліна Геннадіївна, Малюга Олександр Сергійович. Використання штучного інтелекту у вищій освіті: стан і тенденції. International Science Journal of Education and Linguistics. Vol. 3, No. 2, 2024, pp. 27—35. URL: https://doi.org/10.46299/j.isjel.20240302.04 (дата звернення: 23.02.2025).

РОЗДІЛ 8
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Юрій ЛИСЕЦЬКИЙ,
доктор технічних наук, доцент

8.1. Можливості застосування штучного інтелекту у сфері кібербезпеки

З огляду на величезні обсяги даних, з якими доводиться працювати сьогодні, і брак досвідчених фахівців з кібербезпеки, багато організацій вже використовують можливості ШІ для забезпечення кібербезпеки [1]. Передбачається, що ШІ, перебравши на себе більшу частину рутинних процедур, звільнить фахівців від простих і складних завдань. Так, наприклад, ШІ може аналізувати події у сфері кібербезпеки, виявляти відхилення від норми в роботі програм та пристроїв і сповіщати про це співробітників служби кібербезпеки [2].

За оцінкою MarketsandMarkets, в 2019–2026 рр. ринок засобів ШІ для забезпечення кібербезпеки зростатиме в середньому на 23,3% за рік, з 8,8 до 38,2 млрд. доларів (рис.8.1).

ШІ активно використовується для вирішення питань кібербезпеки на багатьох рівнях. Сучасні системи ШІ здатні аналізувати величезні обсяги даних

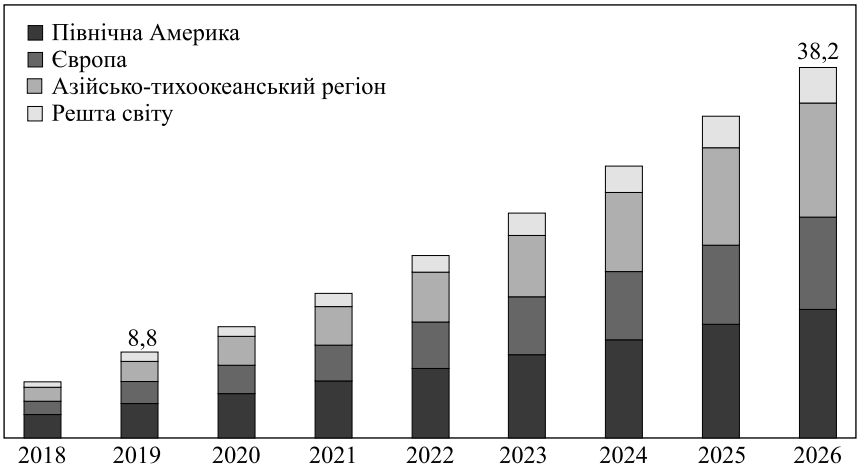


Рис. 8.1. Динаміка зростання ринку засобів ШІ для забезпечення кібербезпеки по регіонах, *млрд дол.*

швидше, ніж людина, і виявляти складні шаблони або аномалії, які можуть вказувати на потенційні загрози. ШІ застосовується також для підвищення ефективності захисту кінцевих точок, таких, як антивіруси та фаєрволи, що дає можливість передбачати і блокувати їх атаки заздалегідь. Основні напрями застосування ШІ у сфері кібербезпеки [3]:

прогнозування загроз. ШІ може допомогти ідентифікувати потенційні нові вразливості та кібератаки до того, як вони стануть серйозними проблемами;

автоматизація відповідей на інциденти. ШІ може автоматично реагувати на інциденти безпеки, скорочуючи час на їх вирішення;

розумний моніторинг мережі. ШІ дає можливість моніторити мережеву активність і виявляти аномалії, що можуть свідчити про несанкціонований доступ чи вторгнення;

управління ідентифікацією та доступом. Використання ШІ для зміцнення систем управління доступом забезпечує можливість доступу тільки уповноваженим користувачам;

шифрування SSL/TLS. Безпечні протоколи зв'язку, що використовують ШІ, допомагають забезпечити захист даних під час передачі. Зараз ШІ є не просто зручним інструментом, а необхідною складовою системи ефективного захисту від кіберзагроз.

ШІ відіграє ключову роль у прогнозуванні кіберзагроз завдяки своїм спроможностям обробляти великі обсяги даних та виявляти складні зразки поведінки, що зазвичай неможливо в разі застосування традиційних аналітичних методів [8]. У цьому процесі ШІ може допомогти, виконуючи такі функції:

аналіз даних у реальному часі. ШІ може моніторити та аналізувати мережевий трафік щодо аномальних поведінок, які вказують на потенційні кіберзагрози;

автоматизація виявлення загроз. ШІ може автоматизувати процеси виявлення та класифікації загроз, скорочуючи час реакції на інциденти безпеки;

підвищення точності прогнозів. Завдяки машинному навчанню системи на базі ШІ можуть "навчатися" від попередніх атак та вдосконалювати свою здатність до прогнозування майбутніх загроз;

виявлення невідомих загроз. ШІ може допомогти ідентифікувати нові та раніше невідомі кіберзагрози, аналізуючи моделі поведінки, що мають відхилення від норми;

адаптація до нових загроз. ШІ здатний адаптуватися до змін у кіберзагрозах, постійно оновлюючи бази даних і методи захисту.

Використання ШІ не лише допомагає у прогнозуванні та виявленні кіберзагроз, й сприяє забезпеченню більш адекватною та ефективної відповіді на кіберінциденти, зменшенню фальшивих спрацьовувань і зниженню витрат на захист інформаційних систем (ІС).

ШІ може допомогти у вирішенні таких питань:

швидке виявлення інцидентів. ШІ може аналізувати величезні обсяги даних у реальному часі, швидко виявляючи аномалії, що вказують на потенційні кібератаки. Це дає можливість своєчасно реагувати на кіберзагрози;

класифікація і пріоритизація інцидентів. ШІ допомагає визначати ступень небезпеки кіберінцидентів та пріоритизувати відповіді, щоб команди кібербезпеки могли спочатку зосередитися на найкритичніших загрозах;

автоматизоване реагування. Для відомих типів атак ШІ може автоматично запускати процедури відповіді, такі, як ізоляція заражених систем, блокування зловмисного трафіку або скидання паролів, мінімізуючи потенційні збитки;

адаптивне навчання. Використовуючи машинне навчання, системи ШІ постійно "навчаються" на прикладах з кожного кіберінциденту, підвищуючи свою здатність передбачати майбутні кіберзагрози та реагувати на них;

підтримка прийняття рішень. ШІ може надавати рекомендації щодо оптимальних дій для відповіді на конкретні типи кіберзагроз, допомагаючи аналітикам приймати обґрунтовані рішення з питань кібербезпеки;

зменшення фальшивих спрацьовувань. Завдяки точному аналізу даних ШІ може розрізняти легітимну діяльність від справжніх кіберзагроз, зменшуючи кількість хибних тривог і підвищуючи продуктивність роботи команд кібербезпеки.

Застосування ШІ в автоматизації відповідей на інциденти кібербезпеки значно підвищує здатність організацій ефективно захищатися від кіберзагроз, скорочує час реакції на інциденти та забезпечує високий рівень захисту.

ШІ може суттєво поліпшити моніторинг мереж за допомогою автоматизації та підвищення точності аналізу даних. Відзначмо кілька способів, використання ШІ для розумного моніторингу мереж:

автоматизація виявлення аномалій. ШІ може аналізувати патерни мережевого трафіку в реальному часі, виявляючи аномалії, які вказують на несанкціонований доступ або інші види кібератак. Це дає можливість швидше реагувати на потенційні загрози;

підвищення точності прогнозування. Завдяки машинному навчанню ШІ може "вчитися" більш точно прогнозувати потенційні кіберзагрози та аномалії в мережі, зменшуючи кількість хибнопозитивних спрацьовувань;

оптимізація пропускної здатності. ШІ може аналізувати патерни трафіку, щоб оптимізувати використання ресурсів мережі, підвищуючи її ефективність і знижуючи затори;

ідентифікація та класифікація загроз. ШІ може автоматично ідентифікувати кіберзагрози та класифікувати їх за типами на основі аналізу даних, що дає змогу виявляти потенційні ризики для мережі;

автоматизоване відновлення мережі після кіберінцидентів. ШІ може автоматизувати процеси відновлення мережі після кібератак, швидко ізолюючи пошкоджені системи та відновлюючи їх нормальну роботу;

безперервне навчання та адаптація. Системи ШІ постійно "навчаються" зі збільшенням обсягу даних, що дає їм змогу адаптуватися до нових загроз і тактик кібератак.

Використання ШІ для розумного моніторингу мереж забезпечує більш глибокий і точний аналіз даних, допомагаючи виявляти кіберзагрози і відповідати на них більш ефективно та з меншими витратами ресурсів.

ШІ може суттєво вдосконалювати процеси ідентифікації та доступу за багатьма параметрами, зокрема:

розпізнавання облич. ШІ може використовувати біометричні дані для розпізнавання осіб та надання доступу до системи або приміщень;

аналіз поведінки користувачів. Застосування алгоритмів машинного навчання для аналізу звичних дій користувачів допомагає ідентифікувати підозрілі дії, що можуть свідчити про неавторизований доступ;

автоматичне управління доступом. ШІ може автоматизувати процеси надання чи відкликання доступу, базуючись на визначених критеріях, таких, як рівень безпеки, час входу та ін.;

виявлення шкідливого ПЗ. ШІ може виявляти та блокувати шкідливе ПЗ (ШПЗ), за допомогою якого зловмисники намагаються дістати несанкціонований доступ до ІС;

посилення кіберзахисту. Інтеграція ШІ в системи ідентифікації може посилити кіберзахист, оскільки ШІ постійно навчається та адаптується до нових методів атак;

інтеграція з іншими системами. ШІ легко інтегрується з різними системами управління ідентифікацією та доступом (Identity and Access Management, IAM), підвищуючи ефективність управління ідентифікацією.

Використання ШІ в системи управління ідентифікацією та доступом може дати організаціям перевагу у швидкості, точності та ефективності захисту своїх ІС. ШІ може зіграти ключову роль у посиленні безпеки протоколів зв'язку, як-от SSL/TLS, які використовуються для шифрування даних під час їх передачі через мережу. Він може це зробити кількома способами:

виявлення аномалій. ШІ може аналізують шаблони трафіку мережі і виявляти відхилення, які вказувати на спроби злому системи шифрування або інші кібератаки;

автоматичне оновлення та підтримка. ШІ може допомагати в забезпеченні актуальності протоколів, автоматизуючи процес оновлення криптографічних ключів та сертифікатів безпеки;

машинне навчання для прогнозування. Застосування технік машинного навчання для прогнозування та виявлення потенційних зламів до того, як вони стануться, що дає можливість проактивно захищати ІС;

автоматизоване тестування безпеки. ШІ може здійснювати складне тестування безпеки протоколів для виявлення слабких місць та вразливостей у шифруванні даних;

підтримка складних систем. ШІ може підтримувати більш складні системи шифрування, які є занадто важкими для ручного управління.

У використанні ШІ для підтримки безпечних протоколів зв'язку ключовим елементом є постійне вдосконалення технологій й адаптація до нових загроз. ШІ забезпечує можливість масштабування й адаптації, що необхідно для захисту даних у сучасному цифровому світі.

ШІ відкриває нові горизонти у сфері кібербезпеки, але разом з тим він може створювати і серйозні загрози [4]:

автоматизація атак. ШІ можна використовувати для створення і проведення швидких та ефективних кібератак, які важко виявляти та блокувати традиційними методами;

поліпшення фішингових атак. За допомогою ШІ фішингові атаки можуть стати більш переконливими, оскільки вони здатні імітувати патерни людського письма і поведінки;

використання у глибоких підробках (deepfake). ШІ може створювати дуже реалістичні аудіо- і відеопідробки, що сприяють поширенню дезінформації та впливу на громадську думку або індивідуальні рішення;

маніпулювання даними. ШІ можна використовувати для маніпулювання даними або їх зміни без виявлення, що може мати серйозні наслідки для збереження цілісності інформації;

створення нових видів вразливостей. Інтеграція ШІ в системи кібербезпеки може також відкрити нові вразливості, які можуть бути використані зловмисниками;

автономні кіберзброї. Використання ШІ у створенні автономних кіберзброй може призвести до необоротних атак, які можуть бути запущені без людського втручання.

Отже, ключ до захисту проти цих загроз полягає в розробці комплексних стратегій кібербезпеки, які передбачають використання ШІ як інструменту захисту, а також як потенційної мішені для захисту. Для забезпечення кібербезпеки за допомогою ШІ потрібно більше кваліфікованих експертів. Ефективність засобів мережевої безпеки, основаних на ШІ, стане набагато вище за наявності фахівців, здатних обслуговувати і налаштовувати їх у міру потреби.

8.2. Побудова операційної системи кібербезпеки з використанням штучного інтелекту

Одним зі сучасних світових трендів є суттєве зростання кількості кібератак, які стають все більш витонченими і малопрогнозованими. Особливою метою кіберзлочинців є критично важливі об'єкти інфраструктури країни. Так у червні 2017 року відбулася найбільша кібератака в історії країни вірусом-шифрувальником Petya.A, що заблокувала роботу тисяч українських компаній та державних органів [5]. 12 грудня 2023 року відбулася наймасштабніша в історії глобального телекомринку кібератака на мережу "Київстар", яка забезпечує послугами мобільного зв'язку близько 50% абонентів України, зокрема державні установи й силові структури [6]. А 9 грудня 2024 року відбулася наймасштабніша за останній час зовнішня кібератака на державні реєстри України. Було призупинено роботу Єдиних та Державних реєстрів, які перебувають у компетенції Міністерства юстиції. Через атаку на державні реєстри у "Дії" тимчасово стали недоступними 27 послуг, зокрема реєстрація ФОП та ТОВ, бронювання працівників від мобілізації, перереєстрація авто, реєстрація права власності на майно, оформлення допомоги

дітям, “єОселя”, “єВідновлення”, подання заяв про шлюб тощо. Сервісні центри Міністерства внутрішніх справ також тимчасово призупинили надання окремих реєстраційних послуг, пов’язаних зі зміною власника транспортного засобу [7]. Держава виявилася не в змозі протистояти таким атакам, тому для захисту від інформаційних та кіберзагроз потрібні нові технології та системи і питання створення ефективних засобів кіберзахисту є дуже актуальним [8].

На теперешьний час, одним із найсучасніших засобів захисту корпоративного рівня є Security Operation Center (SOC). Сьогодні в Україні вже існує кілька SOC, зокрема і комерційних, але питаннями їхньої побудови також цікавляться інші державні організації та підприємства практично всіх галузей вітчизняної економіки [9]. Цей інтерес викликаний насамперед кібератаками, що постійно вдосконалюються, і потребою в сучасних засобах протидії. Дійсно, SOC є ефективним засобом забезпечення інформаційної та кібербезпеки будь-якої організації, що дозволяє здійснювати моніторинг, детектування та оперативну реакцію на інциденти безпеки. Слід зазначити, що побудова SOC потребує чималих матеріальних витрат і не всі організації можуть собі їх дозволити. Тому питання створення аналогічного, але менш дорогого засобу допомогло б розв’язати цю проблему.

Проведений аналіз наявності та експлуатації промислових систем інформаційної та кібербезпеки вітчизняними організаціями корпоративного рівня показав, що в середньому використовується понад 20 класів таких систем (рис. 8.2).

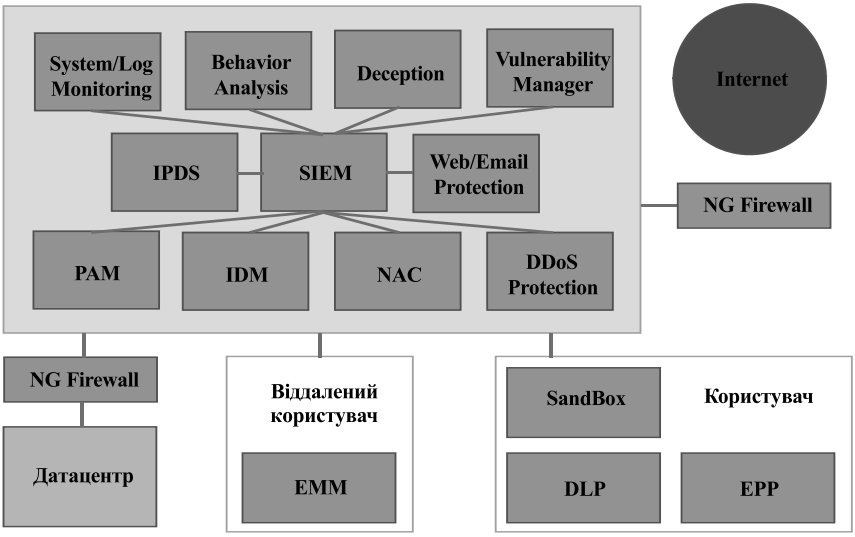


Рис. 8.2. Системи корпоративної інформаційної та кібербезпеки організації

Рис. 8.3. Компоненти кібербезпеки

Це не означає, що всі вони обов'язково мають бути впроваджені для досягнення "повної безпеки", але це демонструє, наскільки широкий "фронт" кібервійни та наскільки можна формувати ландшафт кібербезпеки, тому що для неї вже є необхідний базис.

Кібербезпека — це захист комп'ютерів, мереж, програмних додатків, критично важливих систем та даних від потенційних кіберзагроз та кібератак. Тобто займається збереженням корпоративної інформації й можливістю її обробляти, то кібербезпека стосується до таких понять як: віруси, програмні вразливі місця, витік даних, атаки з відмовою в обслуговуванні (DDoS — Distributed Denial of Service attack), вимагання викупу, фішинг та інші, які спрямовані на компрометацію даних, розрив сервісу та крадіжку вираженої інформації.

Кібербезпеку потрібно розглядати, як синергію трьох її компонентів: технічних засобів, процесів та фахівців (рис. 8.3).

Сучасні атаки найчастіше багатовекторні та поетапні, тобто починаються з вибору вектору атаки, який дасть змогу "пройти" периметр і отримати доступ до тієї чи іншої інформаційної системи. Проходження периметра зараз є лише першим етапом атаки, а не її апофеозом, адже давно минув той час, коли надійний периметр вважався гарантією безпеки IT-інфраструктури, та й саме поняття периметра інформаційної безпеки втратило свою цілісність та монолітність, внаслідок тенденцій розвитку сучасних технологій.

З огляду на це неурядова організація MITRE Corporation розробила модель ATT&CK, що описує поетапність, процес та техніки атак та компрометації корпоративних мереж [10]. Згідно з цією моделлю, процес вторгнення та виконання шкідливих дій складається з декількох етапів, які зображено на рис. 8.4.

Якщо не брати до уваги стадію підготовки, то атака складається з кількох етапів, які включають: доставлення шкідливого вмісту, зараження, взяття

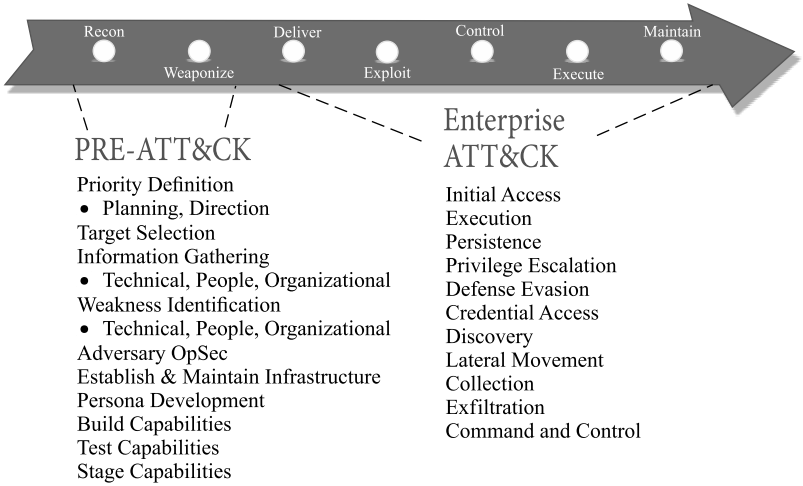


Рис. 8.4. Модель ATT&CK

атакованої системи під управління, виконання руйнівних дій, закріплення та розширення.

За інформацією від компанії-виробника Cisco Systems — світового лідера в галузі мережевих технологій, тривалість злому до проникнення складає хвилини, до виконання шкідливих дій можуть проходити хвилини, години, а часом дні, а ось до виявлення проникнення та результатів атаки минають тижні, місяці, а іноді роки. З огляду на це після того, як нападник, пройшовши периметр, вже проник всередину IT-інфраструктури, захист має одиниці-десятки хвилин на те, щоб запобігти шкідливим діям, а при концепції безпеки, яка все ще існує, орієнтованій на захист периметра, до виявлення проходять місяці, а іноді й роки.

Для того, щоб встигнути відреагувати на дії зловмисника всередині периметра необхідно:

- уповільнити зловмисника, створивши для нього велику кількість помилкових цілей-приманок в IT-інфраструктурі;
- відстежувати активні чи шкідливі дії щодо створених приманок;
- зібрати максимально можливу інформацію про мережевий трафік усередині периметра для пошуку нетипової поведінки;
- зібрати журнали та події IT-підсистем, зокрема інфраструктурних та особливо підсистем безпеки;
- провести нормування, аналіз та кореляцію подій та логів;
- виявити нетипову або небезпечну поведінку та провести розслідування та усунення інциденту.

Виходячи з вищеописаного, для своєчасної реакції на вторгнення, коли периметр уже подоланий зловмисниками, крім наявності стандартних засобів

безпеки (антивірус/EPP/EDR, міжмережевих екранів наступного покоління, систем безпеки електронної пошти та доступу до WEB, систем керування доступом до мережі тощо) для ефективного відображення сучасних атак необхідний збір та централізований аналіз подій усередині IT-інфраструктури. Зважаючи на те, що в мережі середніх розмірів обсяг записів про події за добу може досягати десятків гігабайт, перегляд цих подій та їх аналіз є дуже трудомістким, що посилюється різною структурою повідомлень, різними рівнями критичності тощо. Саме для цих цілей використовуються системи Security Information and Event Management (SIEM), завданням яких і є збір логів із систем, їх нормалізація, знаходження підозрілих дій і залежностей для повідомлення про них фахівцю з безпеки, як про подію (вдалий, невдалий або тривалий злом).

Але будь-який засіб збору та аналізу інформації не є ефективним, якщо недостатньо даних для аналізу. На вхід аналітичного інструментарію має надходити інформація про різні події та процеси в IT-інфраструктурі. Особливо цінна інформація про мережеву активність, про знайдене ШПЗ, про спрацювання правил безпеки модулів запобігання вторгненням, а також про спрацювання пасток-приманок.

Для вирішення цього завдання необхідно визначити мінімально необхідний набір систем та пристроїв, який дасть можливість забезпечити базовий рівень безпеки IT-інфраструктури. Безумовно, базовий — "виконавчий" набір систем кібербезпеки повинен бути присутнім в IT-інфраструктурі організації. Термін "виконавчий" акцентує на тому, що ці системи виконують кожну свою роль у розв'язанні задачі кіберзахисту і при цьому вони не забезпечують додаткового інтелекту, що інтегрує або аналізу, а просто захищають конкретні типи систем від конкретних типів атак. До списку таких обов'язкових систем належать:

- Next Generation Firewall (NGF);
- Endpoint Protection (EPP)/Antivirus або Endpoint Detection&Response (EDR);
- System/Log Monitoring;
- Netflow Analyzer;
- Threat Intelligence;
- Deception.

Це базовий набір, і він може бути розширений залежно від специфіки IT-інфраструктури організації та функціональних завдань. Ці ж системи, крім своїх прямих функцій, генерують і передають в аналітичну/корелюючу систему, інформацію про специфічні події безпеки саме для цієї системи кібербезпеки для об'єднання в єдину базу даних (БД) і виконання аналізу.

Як централізоване аналітичне ядро системи корпоративної кібербезпеки, виступає система збору та аналізу логів та подій — SIEM, яка збирає події з доступного набору систем, нормалізує їх та проводить аналіз, кореляцію сукупностей подій, а також надання команді кібербезпеки результатів аналізу у вигляді рекомендацій, висновків та подій.

Для розуміння процесів, що відбуваються в мережі організації, дані про трафік (включаючи дані про 4-й рівень моделі OSI) треба знімати не тільки з прикордонних маршрутизаторів та NGF, але і з мережевих пристроїв у вузлових точках, а для розуміння процесів у всіх сегментах — бажано з усіх мережевих пристроїв. Прикладом можуть бути дані, одержані Netflow, причому необхідна інформація про всі пакети, а не Sampled варіант. Збирати та аналізувати всю первинну інформацію NetFlow безпосередньо в SIEM або попередньо виконувати передобробку Netflow на collector/analyzer, або використовувати для аналізу систему типу Threat Intelligence з підключенням Behavior Analysis та хмарних аналітичних систем залежить від наявного IT-ландшафту, завдань, обсягу мережі та типу/інтенсивності трафіку та вибирається на етапі проєктування.

Для обробки та кореляції подій та процесів в IT-системах (сервера, системи збереження даних (СЗД), операційні системи, додатки, тощо) необхідне оброблення журналів подій з додатків, гіпервізорів, БД, апаратних платформ тощо. Для цього такі події можуть направлятись у SIEM безпосередньо та може здійснюватися збір та передообробка у syslog або SNMP серверах. Для виявлення ознак успішного вторгнення в мережу та ідентифікації шкідливого коду використовуються системи класу “пастки”, які провокують зловмисника на активні дії проти створеної обманної псевдосистеми, яка має всі ознаки “жертви”, але при цьому невідома легітимним користувачам і потрібна лише для того, щоб відстежувати спроби атак на неї та повідомляти системі кібербезпеки деталі про зловмисників та про тип/спосіб атаки. З погляду запобігання злому IT-систем, дуже ефективним способом є аналіз IT-систем на відомі вразливості з допомогою систем класу “сканер вразливості”. Таке періодичне сканування дає можливість визначити, які із систем потенційно вразливі для тих чи інших класів атак та завчасно вжити заходів для захисту.

Очевидно, що чим більше IT-систем будуть передавати інформацію про події та активності на систему кібербезпеки, тим більш комплексний аналіз буде виконано і більше кореляційних правил буде застосовано, а це своєю чергою дозволить команді безпеки забезпечити повну “видимість” процесів в IT-інфраструктурі організації та дій зловмисників. Для визначення потенційного інциденту кібербезпеки, як зазначалося вище, необхідно провести аналіз та кореляцію по великій кількості подій та даних, які дадуть можливість отримати повну картину процесів та подій. З боку аналізу подій в кібербезпеці, саме методи обробки BigData на предмет виявлення аномалій у поведінці користувачів, подій або трафіку відповідають концепції штучного інтелекту/машинного навчання (artificial intelligence/Machine Learning, AI/ML).

Ця технологія демонструє дуже високу ефективність у задачах визначення аномалії у будь-яких послідовностях або масивах даних. ML використовується для визначення підозрілої аномалії будь-якої природи та для аналізу наявності або вірогідності потенційної атаки на основі визначених подій, фактів, трендів та аномалії

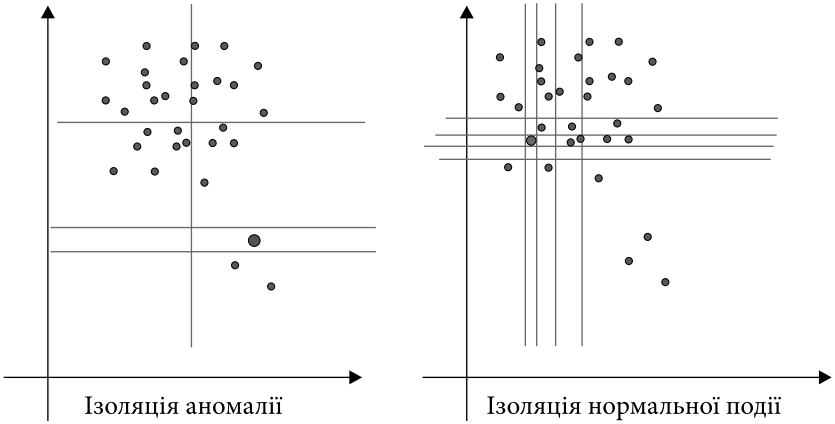


Рис. 8.5. Обробка інформації в режимі квазіреального часу за методом Isolated Forest (IForest)

Для реалізації задачі визначення:

- аномалій у трафіку корпоративної мережі;
- аномалій у трафіку Інтернет (визначення та боротьба с DDoS атаками);
- аномалій у поведінці користувачів

використовується метод машинного навчання без вчителя. Система збирає дані за певний час та будує профіль поведінки кожного користувача або трафіку, яке розглядається як норма, щодо якої визначається аномалія.

Ця інформація оброблюється в режимі квазіреального часу за методом Isolated Forest (IForest) чи Extended Isolated Forest (рис.8.5).

Відповідно до типу оцінюваної аномалії задають гіперпараметри — кількість “дерев” у “лісі”, глибина “дерева”, передбачувана доля аномалії у наборі даних, мінімальна вибірка до розділення та ін. Ці гіперпараметри задані у системі та можуть підбиратися шляхом аналізу, як результат процесу перебору, але адміністратор також може змінювати їх залежно від наявного ландшафту.

Використання ML для аналізу подій та даних або виявлених аномалії з метою визначення ймовірної атаки (інциденту кібербезпеки) грунтується на матриці MITRE ATT&CK, яка класифікує атаки та описує їх з точки зору векторів атаки та засобу використання їх для здійснення атак (розділ Detection).

Після обробки матриці MITRE ATT&CK, система ML отримує нормалізовану матрицю великої кількості атак, яка використовується як ландшафт для роботи моделі. Також система отримує з аналітичних систем та систем кібербезпеки події, які визначені системою з вірогідністю, заданою відповідним гіперпараметром алгоритму, та використовує їх як ознаку/характеристику для моделі. Задача алгоритму використати ознаки (поточні факти та

події) з урахування їх вірогідності для класифікації вірогідної атаки (за матрицею MITRE ATT&CK) та визначити її вірогідність. Після визначення вірогідності певного інциденту кібербезпеки (*Pi*) визначається пріоритет (*Pr*), тобто можлива небезпека цього потенційного інциденту з урахуванням наперед заданого індексу небезпеки інциденту (*Pv*)

$$Pr = 1 - (1 - m \cdot Pi) \cdot (1 - m \cdot Pv)$$

де:

Pr — пріоритет інциденту (діапазон: 0 — 1, більше — важливіший);

Pi — вірогідність наявності певного інцидРієнту (діапазон: 0 — 1);

Pv — індекс небезпеки певного інциденту (діапазон: 0 — 1, більше — небезпечний);

m, n — відповідні вагові коефіцієнти, гіперпараметри.

Далі отримані пріоритети ранжують за методом скорингу та k найбільш пріоритетних інцидентів надають на розгляд команди SOC, а також у наперед заданих випадках (конкретних типах або в залежності від рівня *Pr)*, коли висока вірогідність критичної небезпеки, запускають автоматизовану послідовність реакції на атаку в системі оркестрації та автоматизації реакції на інциденти (SOAR).

Таким чином, використання систем машинного навчання для визначення та пріоритизації інцидентів кібербезпеки дозволяє різко знизити кількість подій безпеки, які треба обробляти команді SOC, при цьому наявність інциденту визначається штучним інтелектом серед кількох тисяч потенційних інцидентів з урахуванням всій доступної інформації про події, тренди та факти, а не залежить тільки від написаного кореляційного правила або досвіду аналітика SOC. Переважно використання системи штучного інциденту для обробки такого великого масиву даних в кілька етапів з виявлення аномалії та визначення вірогідності настання одного або кілька інцидентів серед багато тисяч потенційних потребує значної обчислювальної потужності. Тому для апаратного забезпечення ОСК необхідно аналіз та розробку, переважно на базі серверів з кількома графічними адаптерами (GPU), на яких найчастіше й оброблюються алгоритми AI/ML.

Ще одним компонентом кібербезпеки є процеси та процедури, які чітко описують для кожного члена команди кібербезпеки дії та подальші кроки у разі тієї чи іншої ситуації, таймінг та рівні ескалації, процедури взаємодії та залучення фахівців.

Процеси та процедури в службі корпоративної кібербезпеки, як і в будь-якій службі швидкого реагування, спрямовані насамперед на швидке та ефективне усунення інциденту та його наслідків, а по-друге, що не менш важливо, на підготовку команди та IT-інфраструктури до роботи в постійно мінливих умовах, і тому діляться, щонайменше, на три типи документів: Emergency, Routine, Escalation для кожної укрупненої ролі фахівців у команді.

Саме фахівці є найціннішим активом будь-якої служби кібербезпеки, недарма зараз у світі спостерігається стійкий дефіцит цих фахівців, який

за деякими оцінками у 2025 р. досягне 4 млн. незаповнених вакансій [11]. Як правило, склад команди кібербезпеки визначається на основі штатного розкладу та формується залежно від обсягу IT-інфраструктури організації, необхідного графіка роботи та вимог до компетенції кожного члена команди.

З урахуванням вищевикладеного, для організації ефективного захисту від кіберзагроз та кібератак, пропонується розроблена архітектура Операційної Системи Кібербезпеки, яка дає можливість здійснювати збір, нормалізацію та кореляційний аналіз подій в IT-інфраструктурі організацій, а також автоматизувати процес розслідування кіберінцидентів та реакції на атаки [12]. ОСК має такі складові (рис. 8.6) :

• програмно-апаратний комплекс (ПАК) аналітичної платформи Splunk Enterprise з модулем Enterprise Security та системою аналітики на бази штучного інтелекту;

• ПАК платформи автоматизації та оркестрації розслідувань і реакції на інциденти Splunk SOAR;

• системи кібербезпеки, що входять до базового — "виконавчого" набору та доналаштовуються при побудові ОСК.

ОСК дозволяє реалізовувати основні процеси, що забезпечують кіберзахист:

♦ збирання логів, Netflow, статистики;

♦ аналіз зібраної інформації та її кореляція;

♦ визначення поточних шкідливих дій;

♦ виявлення можливих атак та підозрілих дій;

♦ формування у автоматичному або автоматизованому режимі реакції на атаки, усунення наслідків атак;

♦ усунення виявлених "проломів" у безпеці.

Впровадження ОСК проводиться в наступній послідовності [13]:

• обстеження наявної IT-інфраструктури організації;

• прояснення та узгодження найбільш небезпечних векторів атак та найбільш уразливих/цінних IT-ресурсів;

• модернізація наявних систем інформаційної і кібербезпеки організації до базового рівня (якщо це потрібно);

• встановлення та інсталяція ПАК збору, нормалізації, кореляції та аналізу подій;

• встановлення та інсталяція ПАК автоматизації та оркестрації розслідувань і реакції на інциденти;

• розробка та впровадження політики, процесів інструкцій, їх адаптація для конкретних умов на всіх етапах моделі ATT&CK (Predict, Prevent, Detect, Response);

• навчання штату IT-безпеки.

Основна перевага ОСК — це можливість отримання інформації про події з різних джерел та їх кореляційний аналіз (200+ кореляційних правил), адже сучасні кібератаки та кіберзагрози можна виявити тільки за сукуп-

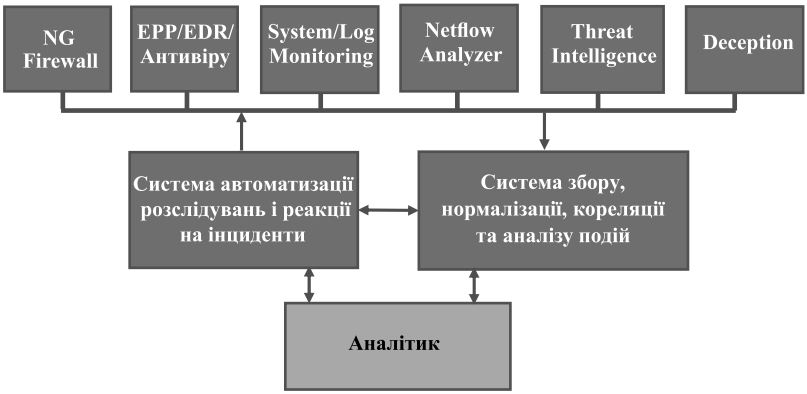


Рис. 8.6. Архітектура ОСК

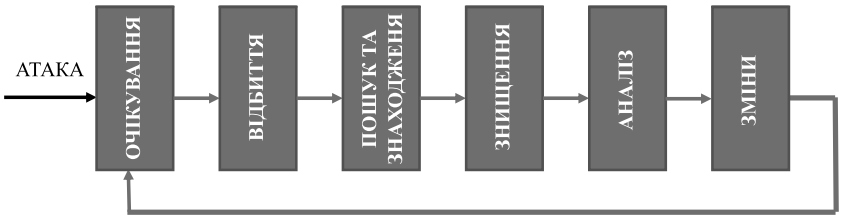


Рис. 8.7. Ітераційний процес адаптації ОСК

ністю подій, що відбуваються в ІТ-інфраструктурі організації та практично неможливо за окремими подіями в окремих системах інформаційного та кіберзахисту.

Необхідно також пам'ятати, що безпека — це не стан, а постійний процес адаптації триєдиної системи (технічні засоби, процеси, фахівці), який здійснюється ітераційно, з метою запобігти або мінімізувати шкоду від впливу кіберінцидентів на функціонування ІТ-інфраструктури організації (рис.8.7).

Отже, запропонована архітектура ОСК дає можливість забезпечити ефективний захист ІТ-інфраструктури організації від кібератак та кіберзагроз, внаслідок отримання інформації про події та інциденти безпеки з різних джерел та проведення їхнього кореляційного аналізу. Водночас суттєво підвищується ефективність аналізу подій безпеки завдяки обробці аналітиком тільки інцидентів безпеки, а не всього потоку журналів подій і Netflow.

Також: доступна повна "видимість" процесів та подій в ІТ-інфраструктурі організації; з'являється можливість аналізувати та локалізувати інциденти безпеки як усередині, так і на периметрі мережі; істотно підвищується швидкість реакції та обробки кіберінцидентів завдяки використанню сис-

теми автоматизації розслідування і реакції на інциденти та роботі команди згідно з розробленими й адаптованими інструкціями та протоколами, з чіткими ролями. Крім того, при функціоналі ОСК аналогічному функціоналу SOC, вартість її побудови на 15–20% дешевше, а термін впровадження на 2 місяці менше.

8.3. Розробка корпоративної системи кібербезпеки з використанням штучного інтелекту

Сьогодні, коли кіберзагрози стають все складнішими та поширенішими, організації мають виявляти підвищену активність у забезпеченні безпеки. З удосконаленням кіберзлочинців, які використовують як технологічні, так і людські вразливості, тому організаціям важливо випереджати потенційні атаки, а цю можливість має давати система кібербезпеки корпоративного рівня [14]. При цьому як результат забезпечується захист корпоративної інформаційної системи (КІС) організації від великої кількості різноманітних загроз, безперервність процесів електронної обробки інформації, мінімізуються порушення їх функцінування та життєдіяльності [15]. Тому розробка корпоративної системи кібербезпеки (КСК), що дозволяє забезпечити ефективний захист ІТ-інфраструктури організації від кібератак та кіберзагроз, є дуже актуальним завданням [16].

Раніше вважалося, що наявність міжмережевого екрану (ММЕ) вирішує майже 90% проблем, пов'язаних із можливими атаками на КІС і для базового рівня захисту достатньо МСЕ наступного покоління на периметрі та антивірусів, встановлених на робочих станціях та серверах [17]. Однак, поряд із зростанням цінності вмісту КІС, збільшення залежності від даних та їх доступності, зростає і попит на розвиток технологій, методів та засобів кібератак. Сьогодні арсенал засобів та способів отримання чи знищення інформації в КІС величезний та оновлюється щодня. Крім класичних засобів, що дають можливість продіагностувати віддалену систему та виявити її можливі слабкі місця, а також здійснити мережеву атаку в лоб, через шлюз в Інтернеті або за допомогою ШПЗ. З'явилися: комплексні атаки, які здійснюються через кілька векторів атак, не викликаючи підозр у вищеописаних систем кіберзахисту; різні варіанти прихованих шкідливих програм, зокрема безфайлове ШПЗ, що проникає через поштові системи та Web-сесії, що маскуються у зображеннях тощо.

Тому сучасна КСК має включати компоненти, що виконують різні функції і доповнюють один одного, зокрема: захист мережного рівня; захист робочих станцій та серверів; захист даних, що зберігаються та оброблюються в КІС; аналітичні системи кібербезпеки.

До систем захисту мережевого рівня відносять такі: міжмережеві екрани наступного покоління (NGFW); мікросегментація, зокрема у віртуальній інфраструктурі; системи керування доступом до мережі (NAC); віддалений доступ з нульовою довірою (ZTNA); системи захисту від розподілених атак

типу «відмова в обслуговуванні» (DDoS); системи захисту від атак на портали (WAF); брокери безпечного доступу до хмар (CASB.)

До систем захисту робочих станцій та серверів відносять такі: системи захисту від ШПЗ, зокрема від невідомого раніше; система захисту від атак через електронну пошту; система керування мобільними пристроями (EMM/MDM); система управління ідентифікацією та авторизацією користувачів та обліковими записами (IAM); система керування привілейованим доступом; системи захисту фізичного доступу.

До систем захисту даних відносять: системи захисту від витоку інформації (DLP); система багатофакторної автентифікації та авторизації (MFA); системи резервного копіювання та відновлення та системи архівації; системи захисту БД.

До аналітичних систем кібербезпеки відносять такі: система аналізу вразливостей; система аналізу аномалій в мережі чи поведінки користувачів система імітації атак; система кіберпасток; система збору, кореляції та аналізу журналів та дій (SIEM); система автоматизації дій під час розслідування чи реакції на інцидент.

Надалі розглянемо існуючі промислові системи і технології, які використовують для забезпечення кібербезпеки:

1. Міжмережевий екран наступного покоління (NGFW). Як випливає з назви, це пристрій перевірки і фільтрації трафіку, але на відміну від своїх попередників, аналіз трафіку виконується на всіх рівнях моделі OSI аж до сьомого (Application layer), крім безпосередньо функцій ММЕ є також функціонал системи захисту від вторгнень (IPS) та бази даних відомих шкідливих активностей та ресурсів, що оновлюється. Таким чином ММЕ наступного покоління аналізує та фільтрує трафік, використовуючи інформацію про IP адреси, порти тощо аж до додатку, якому належить кожен інформаційний потік. Рішення приймається інтелектуальним двигуном системи на підставі актуальної бази знань. Такі пристрої встановлюють не тільки на периметрі мережі [18], де вони виконують функцію шлюзів безпеки (SWG), а й усередині КІС для контролю трафіку між сегментами та між вузлами КІС. NGFW може бути як апаратними, так і віртуальними, зокрема, працювати на рівні гіпервізора системи віртуалізації контролю трафіку безпосередньо між віртуальними машинами. Необхідність установки NGFW всередині мережі та всередині вузлів аж до рівня віртуальних машин, викликана необхідністю гранульовано розділяти та контролювати трафік для детекції шкідливої активності на ранньому етапі та запобігання розповсюдженню її по мережі. Таке ж завдання вирішує і мікросегментація .

2. Мікросегментація. Мережева технологія, що дає можливість розділити КІС на мінімально можливі логічні мережі, що передають окремі робочі навантаження, і не змішувати трафік, а також контролювати переміщення трафіку між цими логічними мережами називається мікросегментація. І що менше сегменти — то вища швидкість реакцію атаку і менше швидкість її поширення по ІТ-інфраструктурі КІС. З другого краю рівні

моделі OSI можна використовувати, зокрема і VLAN, але як із механізмів такі, як технологія мікросегментації, динамічно налаштовується та функціонує і на другому та третьому рівні моделі OSI, а у віртуальному середовищі на рівні гіпервізора та віртуальних комутаторів.

3. Системи керування доступом до мережі (NAC). Крім завдання поділу та фільтрації трафіку в КІС, стоїть ще завдання визначення та поділу користувачів, які намагаються підключитися до КІС на рівні мережі. Це завдання вирішується за допомогою протоколу IEEE 802.1x, при цьому система контролю та управління доступом до мережі має вміти визначати як хто підключається до мережі за його ідентифікаторами, так й що підключається, тобто, який пристрій [19]. Визначення пристрою (тобто його профілювання) виконується не тільки на базі MAC адреси його мережевого адаптера, але також і за рахунок інших параметрів, так як підстановка коректної MAC-адреси стала вже повсякденною практикою і без детального аналізу робоча станція зловмисника може предстати камерою або сканером з доступом до серверного сегменту. Після відповіді на питання "хто?" і "що?" система приймає рішення "що робити?", а саме чи надавати доступ і, якщо надавати, то куди і з якими правами. Природно, що можливість профілювати пристрій, визначати яке ПЗ встановлено, його версію та налаштування виходить повніше за наявності встановленого на цій робочій станції клієнтського ПЗ системи NAC, яка в разі корпоративних робочих станцій/ноутбуків встановлюється разом з іншим ПЗ.

4. Віддалений доступ із нульовою довірою (ZTNA). Різке зростання кількості працівників, які працюють віддалено і потребують підключення до інформаційних ресурсів КІС, призвело до двох результатів: класичний периметр організації ще більше розмився і зросла роль інших засобів безпеки, важливість системи безпечного, зручного та функціонального віддаленого доступу до ресурсів КІС різко зросла. Класична організація віддаленого доступу з допомогою IPSec VPN часто незручна і потребує великої кількості додаткових систем безпеки наближення до рівня контролю співробітників усередині периметра, оскільки у класичному вигляді вкрай складно контролювати ПЗ встановлене на віддаленому ПК, його захист від Інтернету тощо. Впровадження технології/рішення ZTNA дає можливість організовувати безпечне підключення до ресурсу або додатку КІС за рахунок автоматичної побудови шифрованого тунелю або тунелів до ресурсу або додатку, контролю наявності, версії та функціональності програмного забезпечення або налаштувань на віддаленій робочій станції. Найчастіше рішення реалізовано на проміжному шлюзі, який проводить аутентифікацію/авторизацію та перевірку робочої станції та користувача, а також визначає можливість підключення до тих чи інших ресурсів. Ефективні рішення цього класу мають можливість періодично, в рамках сесії, контролювати виконання умов допуску до ресурсів та змінювати авторизацію у разі, якщо умови перестали виконуватись — процедура Change of Authorization (CoA). Дане рішення функціонально дуже схоже на розглянуте раніше систему управління доступом до

мережі (NAC), але контролює віддалений доступ до ресурсів КІС і працює на інших протоколах та інших технічних реалізаціях.

5. Системи захисту від розподілених атак типу "відмова в обслуговуванні" (DDoS). Однією з найпоширеніших атак сьогодні є атака типу "відмова в обслуговуванні" [20]. Переважно зустрічається розподілена версія атаки, яка здійснюється з тисяч IP адрес. Суть атаки у спробі перевищити пропускну здатність каналу, продуктивність шлюзу, продуктивність ІТ-систем (серверів, СЗД, тощо) завдяки генеруванню, зазвичай з багатьох джерел, великої кількості трафіку у вигляді хибних запитів, сміттєвих даних або спеціальних пакетів, що потребують для її обробки надмірної продуктивності. Для розуміння можливостей таких атак можна сказати, що в 2023 р. на Google була здійснена атака обсягом 298 млн. запитів у секунду, що більше ніж кількість запитів до Wikipedia за весь вересень 2023 р. Незважаючи на те, що автори таких атак бувають дуже винахідливими в способах обходу захисту, більшість атак досить прості, їх дешево організувати і вони просто генерують велику кількість сміттєвих даних у спробі переповнити канал, процесор шлюзу або MME. Якщо КІС для успішного функціонування необхідний доступ до зовнішніх ресурсів в Інтернеті/хмарі або навпаки доступ зовнішніх користувачів до ресурсів КІС, а також, якщо об'єднання вузлів КІС відбувається за допомогою шифрованих тунелів в Інтернет, то DDoS атаки можуть бути згубними для роботи КІС і для функціонування підприємства в цілому. Крім цього, DDoS атаки можуть перевантажувати деякі елементи захисту, що низка виробників може бути вимушена пропускати трафік без контролю перевантаженого пристрою. Можливий також пропуск командою безпеки підозрілих подій внаслідок перемикання уваги на відображення атаки DDoS. Беручи це до уваги, захист від DDoS атак є дуже актуальним завданням і вирішується як на рівні хмарних центрів очищення, так і на рівні сервісів операторів та локальних пристроїв захисту на периметрі КІС. Найбільш ефективні системи захисту від атак DDoS використовують системи штучного інтелекту або машинного навчання з використанням методу "навчання без вчителя". При цьому система навчається характерному трафіку перші кілька тижнів, а після може виявляти нехарактерні патерни трафіку для більш ефективного виявлення атак, особливо так званих повільних або розумних атак.

6. Системи захисту від атак на портали (WAF). Для забезпечення доступу зовнішніх користувачів до внутрішніх ресурсів КІС необхідно не тільки забезпечити захист від DDoS, але й забезпечити захист самого frontend-порталу (по суті WEB додатку) від специфічних атак на WEB інфраструктуру. Проблематикою захисту від таких атак займається проєкт OWASP, відомий публікацією поточного переліку 10 найбільш актуальних способів атаки на WEB додатки (OWASP Top 10). Захист від атак на WEB-додаток виконує Web Application Firewall, який встановлюється в інфраструктуру КІС після системи захисту від DDoS, шлюзу в Інтернеті, але перед WEB-додатком, що захищається.

7. Брокери безпечного доступу до хмар (CASB). Коли йдеться про інфраструктуру КІС зазвичай приділяють увагу ресурсам усередині периметра мережі, але не завжди звертають увагу на ресурси, розташовані в "хмарі", сподіваючись, що їх захистить оператор хмарної інфраструктури, що не є правильним, особливо з урахуванням кількості та швидкості зростання даних та систем, розташованих у "хмарах", а також відсутності зобов'язань операторів захищати дані користувачів від кібератак будь-якого типу (до речі, про збереження "хмарних" даних теж повинен піклуватися та копіювати їх власник, а не оператор, за рідкісним винятком придбаний сервіс резервування). Існує цілий клас систем захисту ресурсів у "хмарах", найбільш відомих з них брокер безпечного доступу, який контролює права користувача для підключення до мережевих ресурсів виходячи з його автентифікації та поведінкового аналізу, перевіряє безпеку додатка для користувача, забезпечує виявлення хмарних додатків КІС, їх моніторинг та управління на своєму рівні. Для захисту від несанкціонованого доступу система може заблокувати користувача або запропонувати йому пройти ще одну перевірку (використовувати ще один фактор аутентифікації), якщо на підставі впроваджених алгоритмів вважатиме, що його поведінка є аномальною або шкідливою. Ще однією функціональністю CASB є захист даних як від загрози знищення або спотворення, так і від витоку даних (функціональність Data Leak Protection — DLP). Таким чином, CASB, з одного боку, захищає корпоративні додатки та дані в "хмарі" від неавторизованого доступу та впливу на інформацію, а також від викрадення інформації, а з іншого боку — від шкідливого впливу на робочі станції користувачів, а через них і на всю інфраструктуру КІС у разі компрометації хмарних програм та сервісів.

8. Системи захисту від ШПЗ, зокрема від невідомого раніше. Антивірусне програмне забезпечення з'явилося дуже давно (майже 40 років тому) і з того часу еволюціонувало разом із еволюцією шкідливого програмного забезпечення. Важливість цієї системи кібербезпеки у складі комплексу безпеки КІС неможливо переоцінити. Це останній рубіж оборони, якщо всі попередні рубежі не впоралися, і атака досягла своєї мети — обчислювального пристрою з даними. Система боротьби з шкідливим програмним забезпеченням на обчислювальних пристроях зараз представлено двома типами рішень Endpoint Detection & Response (EDR) та eXtended Detection & Response (XDR). Обидві системи забезпечують виявлення відомого ШПЗ з великою ймовірністю та використовують інтелектуальні методи аналізу поведінки, передбачення та перевірки у "пісочниці" досліджуваного ПЗ для виявлення невідомого раніше шкідливого коду. Крім цього, такі системи виконують дії, спрямовані на запобігання шкідливим діям та боротьбу зі ШПЗ. Перевагою сучасних систем є централізація управління детекцією та реакцією для того, щоб інформація (профіль/ознаки/...) про вірус, виявлений на одній робочій станції, повідомляється на агент антивірусного ПЗ на інших робочих станціях для своєчасного виявлення та знищення ШПЗ, коли і якщо

він потрапить на цю робочу станцію. Відмінність EDR від XDR полягає в тому, що XDR для виявлення атаки використовує інформацію, одержувану не тільки від робочої станції, а й від мережевих пристроїв, систем кіберзахисту та відповідних баз знань. Необхідно відзначити, що єдиного формалізованого опису, переліку функцій і характеристик XDR зараз немає, і кожен виробник вкладає в цю абревіатуру своє значення і свій погляд.

9. Система захисту від атак через електронну пошту. Вважається, що зараз електронна пошта є найпоширенішим вектором атак, тобто в більшості випадків брамою кібератаки на КІС стає шкідливе посилання або файл відкритий користувачем в електронному листі. Тому системи захисту електронної пошти від кібератак є одним із найважливіших компонентів кіберзахисту. Система захисту електронної пошти дає можливість: перевірки кожного листа на наявність вбудованих потенційно шкідливих експлойтів та їх блокування; блокування листів, отриманих із скомпрометованих або шкідливих доменів; видалення/блокування посилань на шкідливі або підозрілі сайти; видалення з листа шкідливих файлів та файлів налаштованого типу/розширення; передачі до карантину/"пісочниці" підозрілих вкладень або вкладень з певними ознаками; попередження про підозрілий формат, структуру або список адресатів. Цей функціонал побудований на передбачених правилах обробки з можливістю їх кастомізувати та доповнювати командою безпеки КІС з використанням оновлюваних баз знань шкідливих та підозрілих доменів, адрес, структур листа та хешей вкладень. Можливість перевіряти виконувані та офісні файли в "пісочниці" для виявлення потенційно шкідливої поведінки також є потужним інструментом захисту, поряд з інтелектуальним двигуном самого інструментарію. Ще одним рівнем захисту електронної пошти, можливо, найголовнішим, є навчання всіх користувачів основам кібербезпеки при роботі з електронною поштою (часто називають — кібергігієні) і періодичне тестування їх поведінки.

10. Система керування мобільними пристроями (EMM/MDM). Захист мобільних пристроїв, які мають доступ до корпоративних даних від злому або несанкціонованого доступу до інформації, з урахуванням різної способів використання, архітектури та ОС потребує окремих підходів та окремого рішення. На мобільний пристрій встановлюється клієнтське ПЗ системи EMM/MDM, яке створює шифровану область пам'яті, в яку записуються корпоративні програми та дані, доступ до яких здійснюється відповідно до корпоративної політики, встановлюється шифрований тунель в корпоративну мережу, за яким відбувається обмін даними та працюють усі корпоративні програми. Система EMM/MDM відстежує актуальність версії ОС мобільного пристрою та антивірусного програмного забезпечення та контролює налаштування безпеки мобільного пристрою. У разі втрати/крадіжки мобільного пристрою розшифрувати корпоративні дані на мобільному пристрої буде дуже важко, якщо не неможливо, крім того, адміністратор генерує команду на видалення всіх даних корпоративної області та права доступу в корпоративну мережу з пристрою та з бази користувачів КІС.

11. Система керування обліковими записами та авторизацією користувачів (IAM). Однією з можливостей отримати неавторизований доступ до IT-ресурсів КІС є відсутність контролю за життєвим циклом облікових записів та за фактом й історією призначення чи позбавлення прав доступу конкретного співробітника до конкретної системи з конкретними правами. Якщо кількість співробітників обчислюється десятками і немає високої плинності кадрів, то теоретично акуратний адміністратор або співробітник відділу кібербезпеки може вести такий журнал, наприклад, в офісному додатку. Але, якщо кількість співробітників/облікових записів обчислюється сотнями і тисячами та/або висока плинність кадрів, то без спеціальної системи управління обліковими записами та доступом (Identity and Access Management (IAM), дуже велика ймовірність наявності неврахованих та непотрібних прав на доступ до систем та/або активних облікових записів звільнених або перекладених співробітників. Принцип роботи IAM полягає в тому, що IT-системи при спробі користувача до них підключиться, для підтвердження прав користувача на роботу з ними, звертаються до IAM, яка зберігає в собі всі права користувача для роботи з усіма IT-системами компанії, історію їх змін і хто дозволив зміни. Створення облікового запису зі стандартними правами для конкретного підрозділу та посади, зміна прав при переведенні співробітника до іншого підрозділу, а також видалення облікового запису відбувається автоматично на підставі запису у ПЗ відділу кадрів. Для цього система IAM глибоко інтегрується з системою обліку персоналу (відділ кадрів) із системою управління підприємством (ERP) та з корпоративними IT-системами.

12. Система керування привілейованим доступом (PAM). З погляду маніпулювання даними та IT системами, і навіть видалення слідів впливу, системний адміністратор є неконтрольованим тому, що має максимум привілеїв для роботи з системою. Вирішення цієї проблеми покладено на систему, яка може контролювати дії адміністратора та тримати його активності під наглядом команди кібербезпеки та його керівництва. Особливість системи PAM полягає в тому, що її адмініструє команда безпеки і системні адміністратори не мають доступу до її файлів, налаштувань та журналу подій, тобто не можуть впливати на неї. Системи цього класу побудовані як проксішлюз для доступу до адміністрування будь-якої IT-системи. Адміністратори мають права на доступ до системи PAM, але не мають доступу до цільових систем. Після підключення до PAM вони запитують доступ до цільових IT-систем та отримують його після узгодження відповідно до налаштованих правил та ланцюжка авторизації (офіцер безпеки, керівник, запити на уточнення мети тощо). Під час сесії всі дії адміністратора контролюються та зберігаються у кількох форматах аж до відео з метою використання у подальшому розслідуванні. При цьому можливе негайне реагування (припинення сесії, повідомлення тощо) на задані команди або дії, наприклад, спроба введення команди на видалення бази даних або руйнування кластера тощо приведе до блокування сесії та запиту на команду безпеки та керівника.

13. Системи захисту фізичного доступу. Особливість комплексних систем безпеки полягає в тому, що, з одного боку, кібернетична інфраструктура захищається системами контролю фізичного доступу від неавторизованого доступу до IT-обладнання для його фізичного руйнування або для підключення до локальної консолі систем, яка вважається захищеною та надає набагато більше прав на маніпуляцію з системами, ніж через віддалений доступ. А з іншого боку, кіберзахист не дозволяє зловмиснику отримати доступ до систем фізичного захисту (контроль фізичного доступу або відеоспостереження) та внести на них зміни для отримання неправомірної авторизації на фізичний доступ до приміщень КІС. До систем захисту фізичного доступу відносять: різні системи сигналізації на території та в приміщеннях; системи контролю та управління фізичним доступом заснованим на різних способах авторизації та їх комбінаціях (ключ-токен, біометрія (відбиток пальця, малюнок вен, сітківка ока тощо), пароль/код); системи відеоспостереження з функціями відеоаналітики, розпізнавання та пошуку; ситуаційні центри з функцій аналітики комплексних подій та реакції на них.

14. Системи захисту від витоку інформації (DLP). Витік даних можливий не тільки внаслідок кібератак та отримання зловмисниками неавторизованого доступу до даних, а й унаслідок навмисного чи випадкового поширення чутливих даних співробітниками організації. Боротися з цією проблемою покликана система Data Leak Protection (DLP). DLP може мати мережевий та хостовий модуль, які борються з витоками даних на відповідних елементах інфраструктури. Робота системи DLP ґрунтується на класифікації інформації/даних/файлів. Способи класифікації можуть бути побудовані на основі міток у файлах, метаданих, розширення файлів, розташування файлів, входження слів у файл тощо, а також класифікація вручну власником інформації або уповноваженою особою. Сучасні системи DLP можуть попереджати про спробу несанкціонованого поширення інформації, запитувати причини такої спроби для прийняття рішення співробітником безпеки/керівником про дозвіл на цю активність або блокування таких спроб залежно від налаштувань, рівня допуску/дозволу співробітника та ступеня чутливості інформації, але в будь-якому разі, інформація про таку спробу зберігається в журналах системи для можливості аналізу в подальшому.

Найкращі зразки систем DLP запобігають витоку багатьма можливими каналами (реального захисту немає тільки від переписування з екрану на листок і фотографування з екрана не на корпоративний телефон, але це також може бути визначено системою аналітики відеоспостереження, якщо воно розгорнуте в робочій зоні). Серед очевидних та неочевидних каналів витоку: електронна пошта, знімні накопичувачі, мережеві та хмарні файлові архіви, соціальні мережі, месенджери, перетворення на зображення, копіювання інформації з файлу на файл або інше місце, роздруківка тощо. При цьому спрацювання системи DLP далеко не завжди говорить про злий намір, в абсолютній більшості випадків — це ненавмисне порушення полі-

тик співробітниками, що ще раз підтверджує необхідність навчання співробітників основ кібергігієни.

15. Система багатофакторної автентифікації та авторизації. Для зловмисника, однією з найпривабливіших для злому систем на етапі Exploitation/Privilege Escalation послідовності етапів атак Kill Chain є отримання параметрів доступу до важливих робочих станцій чи систем. Отримання будь-яким способом (клавіатурний шпигун, соціальна інженерія, фішинг тощо) імені та пароля дає можливість проникнути всередину КІС і поширюватися до цільових систем. Найпростішим способом перешкодити отриманню доступу до ресурсу мережі таким чином є використання багатофакторної аутентифікації (MFA), яка передбачає для користувача необхідність пройти аутентифікацію кілька разів, використовуючи різні способи/фактори (комбінація імені та пароля, біометрія, одноразовий згенерований пароль (OTP), USB-ключ тощо). Така система захищає від компрометації одного способу доступу, наприклад, від неавторизованого використання USB-ключа зловмисником або підглянутого пароля. Багатофакторна автентифікація робить можливість неавторизованого доступу набагато менш ймовірним і різко підвищує надійність автентифікації та авторизації.

16. Системи захисту БД. Практично у 100% атак метою та найбільшою привабливістю для зловмисників є інформація КІС. У більшості випадків побудови централізованої моделі КІС корпоративні дані зберігаються у відмовостійкому територіально-розподіленому кластері БД. Саме тому отримання доступу до даних, які розташовані в БД, або їх знищення є реальною метою атаки [21]. Це може бути виконано одним із розглянутих вище способів: через вразливі робочі станції та сервери, за допомогою привілейованих облікових записів, через помилки та вразливості в порталі тощо, а може бути використано безпосередньо доступ до БД з урахуванням її особливостей. Тому окремо стоїть завдання захисту безпосередньо систем управління базами даних (СУБД) з урахуванням їх вразливостей, особливостей реалізації та доступу. Функціями систем захисту БД є: прецизійне управління доступами до тих чи інших елементів баз даних або загалом до БД для реалізації моделі рольового доступу користувачів в рамках рекомендацій та законів про захист приватної, медичної та іншої інформації; управління доступами адміністраторів баз даних лише до БД у зоні його відповідальності; контроль коректності, цілісності конфігурації БД та управління її змінами; контроль оновлень СУБД; аудит дій користувачів/додатків та занесення їх до журналу подій; виявлення аномальних активностей у БД та повідомлення про них команду безпеки та/або блокування таких дій, користувачів або програм.

17. Система аналізу вразливостей. Досвідчений адміністратор та співробітник команди безпеки розуміє, що всі реалізації програмно-апаратних рішень мають свої особливості, свої тонкі місця та вразливості, якими може скористатися досвідчений зловмисник для виконання атаки. Одні вразливості "закриваються" виробником рішення черговими оновленнями ПЗ, інші вразливості мають рекомендації щодо заходів щодо запобігання їх вико-

ристанню, треті вразливості поки що не мають ні таких оновлень, ні рекомендацій і просто відомі. Крім того, існують вразливості, для використання яких зловмисники вже розробили ШПЗ, та вразливості, для яких поки що таке ПЗ не випустили або, поки такою вразливістю неможливо або вкрай складно скористатися. Системи аналізу вразливостей якраз і проводять (періодично або постійно) сканування інфраструктури для їх виявлення з наданням звіту за результатами, в якому вказується вразливість, знайдена в конкретному елементі КІС, рекомендації щодо її усунення. Кожній знайденій вразливості надається місце в рейтингу, залежно від серйозності наслідків її експлуатації та можливості скористатися нею для того, щоб команда безпеки пріоритезувала роботи з усунення даних вразливостей, а за неможливості усунути вразливість — купірувала її за допомогою інших систем.

18. Система аналізу аномалій в мережі чи поведінки користувачів. Аналізує непередбачені відхилення у мережі, ІТ системах чи поведінці користувача для передбачення потенційного інциденту кібербезпеки. Такі відхилення або аномалії найчастіше є результатом втручання в роботу систем або мережі та є одним з індикаторів шкідливої активності Для визначення підозрілої аномалії будь-якої природи найбільш ефективно використовувати такі технології штучного інтелекту, як машинне навчання (Artificial intelligence / Machine Learning) (AI/ML). Для реалізації задачі необхідно здійснити визначення: аномалій у трафіку корпоративної мережі; аномалій у трафіку Інтернет (визначення та боротьба с DDoS атаками); аномалій у поведінці користувачів; використовувати метод машинного навчання без вчителя. Система збирає дані за певний час та будує профіль поведінки кожного користувача або трафіку, яке розглядається як норма, щодо якої визначається аномалія. Ця інформація оброблюється в режимі квазіреального часу за методом "ізольованого лісу" (Isolated Forest, IForest) або "розширеного ізольованого лісу" (Extended Isolated Forest).

19. Система імітації атак. Команді безпеки необхідно розуміти наскільки вжиті дії та зусилля захистили інфраструктуру КІС від атак та проникнення. Чи все враховано і чи всі проломи та вразливості закриті (наскільки це можливо). Для цього виконують процедуру "тест на проникнення" (penetration testing), яка виконується командою, яка виконує роль атакуючого зловмисника (red team), ця команда може бути, як складатися із фахівців самого підприємства (якщо вони мають відповідну компетенцію) або це може бути зовнішня команда фахівців у цьому напрямку. Цей тест виконується періодично, раз на рік або раз на півроку. У решту часу команда кібербезпеки підприємства сподівається, що тест був виконаний професійно, і що у них все добре і ніякі нові проломи/вразливості не з'явилися. Альтернативою такого періодичного тестування є використання системи імітації атак (Breach and Attack Simulation, BAS), яка налаштовується на ІТ-ландшафт КІС і запускає набір атак для всіх наявних в КІС ІТ-систем та систем кібербезпеки, а також імітацію атак, розрахованих на слабку ланку захисту — користувача. Такі симуляції атак можуть запускатися так часто, як це може

бути ефективно для даної інфраструктури в автоматичному або автоматизованому режимі. Команда безпеки вивчає підготовлені звіти з рекомендаціями щодо усунення знайдених "дірок" у захисті та виконує "роботу над помилками" з наступним перезапуском симуляції атаки для підтвердження успішного виправлення знайдених проблем.

20. Система кіберпасток. Є статистика, яка показує, що в середньому з моменту проникнення зловмисників у IT-інфраструктуру підприємства до ідентифікації самого факту проникнення проходить понад 20 днів, а до моменту визначення, де і як сталося проникнення, ще більше — 70 днів, причому за останні 5 років ці терміни принципово не змінювалися. Прискорення визначення факту вторгнення та скорочення терміну присутності зловмисників у IT-інфраструктурі для мінімізації збитків і втрат, якщо проникнення все ж таки вдалося, — основне завдання комплексу систем аналітики кібербезпеки. Один із найефективніших засобів виявлення злому є системи кіберпасток (Deception, Honeypot, тощо). Принцип дії цих систем полягає у створенні фіктивних корпоративних IT-ресурсів, вкрай привабливих для зловмисника (каталог AD), БД, поштові сервери, системи управління підприємством, бухгалтерські програми тощо), які мають усі ознаки реальних систем, створюють той самий профіль трафіку, мають ті самі відкриті порти, але при цьому дають можливість себе виявити і підключиться. Факт спроби підключення, а також поведінки після підключення (фіктивний ресурс на відміну від справжнього можна легко виявити в інфраструктурі і він недовго чинить опір злому) сигналізує про те, що в інфраструктуру проник зловмисник. З його поведінки можна зробити висновки про цілі та спосіб проникнення для того, щоб підготуватися до захисту реальних ресурсів і убезпечити дані та постаратися виявити фізично зловмисника, поки він розбирається з фіктивною інформацією на фіктивному ресурсі.

21. Система збору, кореляції та аналізу журналів та дій (SIEM). Для того щоб ідентифікувати спробу злому або шкідливу активність зловмисника в IT інфраструктурі КІС необхідно мати повну видимість всіх процесів у КІС. Для цього необхідно зібрати та проаналізувати багато тисяч записів у журналах подій, події безпеки та велику кількість іншої інформації. У результаті кореляції даних від багатьох IT-систем та систем кібербезпеки може бути виявлений кіберінцидент. Вважається, що тільки таким чином можна виявити сучасні багатовекторні цільові атаки, спеціально розроблені для атаки на дану інфраструктуру. Саме такі атаки прийнято називати цільовою постійною загрозою підвищеної складності (Advanced persistent threat — APT). Нездатність команди кібербезпеки підприємства обробити, проаналізувати та прокорелювати десятки тисяч подій та записів на день призвела до появи системи автоматичного збору, аналізу та кореляції подій в інфраструктурі Security Information & Events Management (SIEM), завданням якої є автоматичний збір подій у системі та аналіз за налаштованими правилами для виявлення потенційного інциденту безпеки та передачі інформації про нього команді безпеки для проведення розслідувань, прийняття рішення про наявність інциденту та

реакції на нього. У періоди між цілеспрямованими масованими атаками на організацію таких інцидентів у середній організації з'являється 2—5 на день, що вже реально розслідувати силами кваліфікованої команди безпеки.

22. Система автоматизації дій під час розслідування чи реакції на інцидент. У розслідуванні інциденту та реакції на нього важливе запобігання або зменшення шкоди від атаки, а значить мінімізація часу присутності зловмисників в інфраструктурі КІС, так як поки команда безпеки ідентифікує та локалізує присутність зловмисника в ІТ, зловмисник продовжує шкідливі дії. У процесі розслідування та реакції на інцидент дуже багато дій є рутинними та характерними для тієї чи іншої атаки чи активності. Наприклад, це можуть бути такі дії: з'ясування атакуючих IP адрес, країни, історію появи та досвід боротьби, схожі атаки на цей же ресурс тощо; а для реакції на них такі: блокування даної IP адреси або поштового домену; видалення або блокування активного контенту та вкладень у всіх листах з даного поштового домену; відправлення файлів, що відповідають низці ознак, на перевірку в "пісочницю", відключення від мережі цієї робочої станції, блокування або зниження прав доступу для скомпрометованого облікового запису, запуск відповідних додатків тощо. Кожна команда безпеки формує сама послідовність дій характерні для тієї чи іншої ситуації. Виконання цих дій автоматично або автоматизовано за командою оператора або спрацьовування тригера появи того чи іншого інциденту дає можливість економити десятки і сотні хвилин у напруженій стадії розслідування та реакції, що може істотно знизити ту шкоду, яку завдає зловмисник. Автоматизацію процесів у кібербезпеці здійснюють системи класу Security orchestration, automation and response (SOAR), які мають велику кількість вбудованих послідовностей дій для більшості стандартних ситуацій, дають можливість налаштовувати та створювати нові послідовності дій. Створення нового набору команд/дій може виконати спеціаліст безпеки без навичок програмування, у графічному інтерфейсі, методом перетягування у правильне місце на схемі відповідних піктограм дій та стрілок умовних та безумовних переходів. Для ефективної взаємодії з ІТ-інфраструктурою та системами безпеки, SOAR мають вбудовану інтеграцію з абсолютною більшістю існуючих ІТ-систем та систем кібербезпеки, які дозволяють SOAR отримувати додаткову інформацію для збагачення події та виконання необхідних дій. Крім того, якщо такої інтеграції немає, то SOAR дає можливість створювати інтерфейси до третіх систем на основі вбудованого інструментарію.

Перераховані вище системи кібербезпеки створюють екосистему корпоративної кібербезпеки у складі чотирьох кластерів: безпека робочих станцій, безпека даних, мережна безпека та аналітика. Вибір необхідних систем кіберзахисту для побудови КСК визначається на етапі проєктування з урахуванням ІТ-ландшафту, структури корпоративної мережі, критичності ІТ-ресурсів тощо. У кожному конкретному випадку склад КСК може відрізнятися відповідно до наявності та важливості тієї чи іншої ІТ-системи. Принципово важливими компонентами є системи щодо захисту мережі типу NGFW, за-

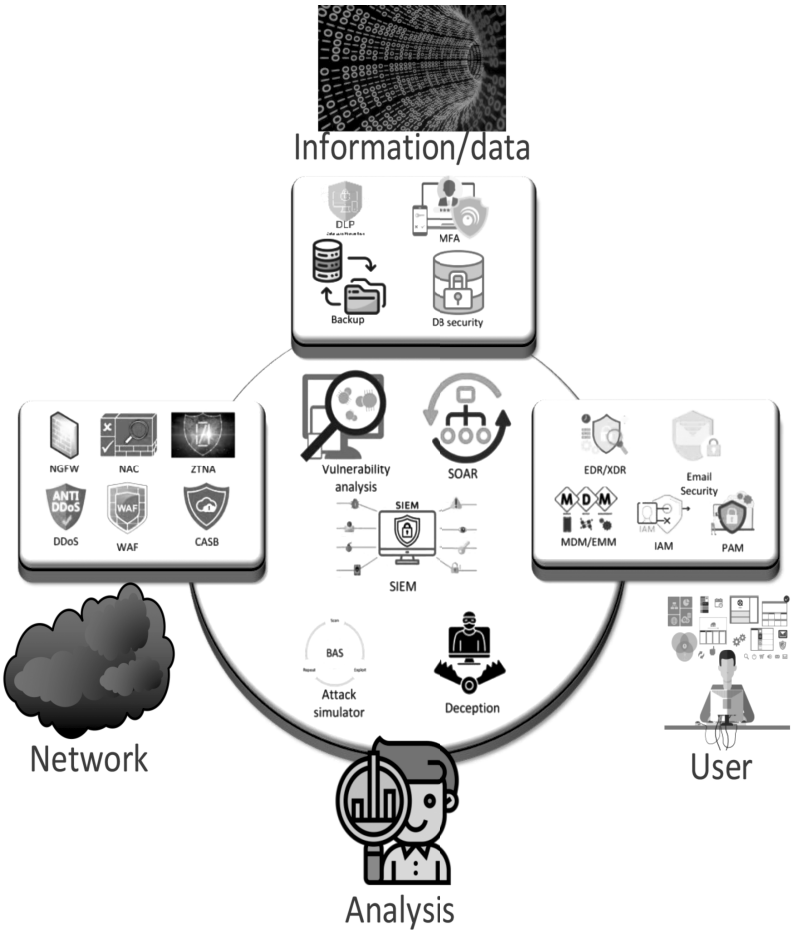


Рис. 8.8. Архітектура КСК

хист робочих станцій і серверів від ШПЗ на базі EDR/XDR, захист системи електронної пошти. Рекомендованими компонентами також є такі: система управління доступом до мережі (NAC) та віддаленим доступом з нульовою довірою (ZTNA), захист від витоків інформації, комплекс систем автентифікації та авторизації.

Рішення про доцільність використання інших систем кібербезпеки залежить від наявності відповідних IT-систем в організації, які потрібно захищати цією технологією кіберзахисту. При цьому для організацій середнього та великого розміру або із середньою чи високою складністю IT-ландшафту системи кластера аналітики кібербезпеки є критично важливими, особливо

системи збору та кореляції подій та система аналізу вразливостей. Така увага системам аналітики приділяється насамперед тому, що багато сучасних атак можна виявити тільки в результаті аналізу подій у кількох системах, при цьому кожна така подія буде в гіршому випадку підозрілою, але не викличе реакції спеціалізованої системи кіберзахисту — фаєрволу, захисту кінцевої точки тощо. Тільки сукупність цих подій може виявити факт здійснення багатовекторної атаки. Також дуже рекомендованою до включення в склад КСІК є система кіберпасток і система оркестрації та автоматизації реакції. Беручи до уваги вищевикладене, архітектура КСК має бути як на рисунку 8.8 [22].

Крім розглянутих технічних засобів захисту від кібератак, суттєва увага повинна приділятися навчанню співробітників та адміністраторів. Вважається, що до 40% атак спрямовані на вразливість людини, так звана соціальна інженерія. Цей термін описує вивчення конкретної людини або групу людей для того, щоб зрозуміти їхню реакцію на запит, підготувати для них найбільш привабливе послання з тим, щоб вони стали точкою проникнення атаки в КІС.

Постійне навчання користувачів кібергігієні, тестування та робота над помилками може бути організовано в автоматизованому режимі за допомогою систем класу Security awareness training system, застосування яких може серйозно підвищити загальну кібербезпеку компанії. Крім того, існують спеціальні навчальні програми та полігони, які дають можливість підвищувати кваліфікацію та напрацьовувати досвід спеціалістам команди кіберзахисту та Security Operations Center (SOC).

Таким чином, сукупність описаних технологій кіберзахисту, правильний вибір необхідних систем захисту від специфічних загроз, побудова аналітичної платформи аналізу подій з використанням ШІ, пошуку загроз та реакції на них, а також постійне навчання співробітників дасть можливість побудувати надійну ешелоновану систему ефективного кіберзахисту КІС. Запропонована архітектура КСК дозволяє підвищити рівень кіберзахисту критичної інфраструктури організації, внаслідок отримання інформації про події та кіберінциденти з різних систем інформаційної і кібербезпеки та проведення їхнього аналізу за допомогою ШІ.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вплив штучного інтелекту на сферу кібербезпеки. URL: https://softico.ua/uk/news/vpliv-shtuchnogo-intelektu-na-sferu-kiberbezpeki/ (дата звернення: 10.03. 2024).
2. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення: 10.03.2024).
3. Лисецький Ю.М., Данченко О.І. Використання штучного інтелекту в сфері кібербезпеки. *Вісник воєнної розвідки*. 2025. № 86. С. 42—45.
4. Загрози та ризики використання штучного інтелекту. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/520 (дата звернення: 12.03. 2024).

5. Від кібератаки вірусом Petya.A постраждали до 10 % комп'ютерів в Україні — Шимків / Новое Время. URL: http://nv.ua/ukr/ukraine/events/vid-kiberatakivirusom-petya-a-postrazhdali-do-10-komp-juteriv-v-ukrajini-shimkiv-1442363.html (дата звернення 01.12.2024).
6. Кібератака зруйнувала близько 40% інфраструктури «Київстару». URL:https://biz.censor.net/news/3463157/kiberataka_zruyinuvala_blyzko_40_infrastruktury_kyyivstaru (дата звернення 22.12.2024).
7. Держреєстри України зазнали наймасштабнішої зовнішньої кібератаки за останній час. URL: https://www.ukrinform.ua/rubric-society/3940051-derzreestri-ukrainizaznali-najmasstabnisoi-za-ostannij-cas-kiberataki-stefanisina.html (дата звернення 20.12.2024).
8. Лисецький Ю.М., Крисяк П.В. Концептуальні основи системи національної кібербезпеки. *Вісник воєнної розвідки*. 2021. № 65. С. 67—72.
9. Лисецький Ю.М., Бобров С.І. Деякі аспекти побудови системи національної кібербезпеки. *Математичні машини і системи*. 2021. № 2. С. 15—22.
10. ATT&CK for Enterprise Introduction URL: https://attack.mitre.org/resources/enterprise-introduction/ (дата звернення 05.12.2024).
11. The Mad Dash to Find a Cybersecurity Force URL: https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html (дата звернення 05.12.2024).
12. Лисецький Ю.М., Молдаван В.Т., Семібаламут К.М. Розробка архітектури операційної системи кібербезпеки. *Вісник воєнної розвідки*. 2024. №78. С. 25—30.
13. Лисецький Ю.М. Побудова операційної системи кібербезпеки з використанням штучного інтелекту. *Вісник воєнної розвідки.* Спеціальний випуск "Штучний інтелект у сфері безпеки і оборони". 2025. С. 50—56.
14. Лисецький Ю.М., Бобров С.І., Данченко О.І. Корпоративна система інформаційної та кібербезпеки. *Математичні машини і системи*. 2024. № 3. С.7—49.
15. Лисецький Ю.М. Забезпечення інформаційної безпеки. Global science: prospects and innovationsи: зб. статей III Міжнар. наук.-практ. конф. (м. Ліверпуль, 2—4 лист. 2023 р.). Великобританія, Ліверпуль, 2023. С. 273–276.
16. Лисецький Ю.М. Комплексная безопасность корпоративных информационных систем. *Управляющие системы и машины*. 2019. № 1. С. 16–22.
17. Міжмережевий екран: що це та як працює? URL: https://ukeywaf.com/baza/mizhmerezhevyj-ekran-shho-cze-yak-praczyuye/ (дата звернення: 10.01.2025).
18. Лисецький Ю.М. Управління доступом до IT-систем. Scientists and existing problems of human development : зб. тез IX Міжнар. наук.-практ. конф. (м. Загреб, 14—17 лист. 2023 р.). Хорватія, Загреб, 2025. С. 378—379.
19. Калбазов Д.І, Лисецький Ю.М. Особливості управління правами користувачів у корпоративних IT-системах. Математичні машини і системи. 2023. № 2. С. 28–33.
20. Лисецкий Ю.М. Информационная безопасность: защита от DDoS-атак. System Analysis and Information Technologies SAIT 2014: 16-th International conf. (Kyiv, 26—30 May 2014). Kyiv, 2014. P. 405—406.
21. Калбазов Д.І., Лисецький Ю.М. Інформаційна безпека корпоративних баз даних. Математичні машини і системи. 2023. № 3. С. 31—37.
22. Лисецький Ю.М. Розробка архітектури корпоративної системи кібербезпеки. *Вісник воєнної розвідки.* Спеціальний випуск "Штучний інтелект у сфері безпеки і оборони". 2025. С. 57—67.

ДЛЯ НОТАТОК

Наукове видання

Алексєєнко І.В., Дзядук Д.О., Кармазіна М.С.,
Лисецький Ю.М., Мокляк С.П., Смолянюк В.Ф., Ткач І.М.

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Монографія

За загальною редакцією Мокляка Сергія Петровича

Літературний редактор, коректор Н.В. Поліщук
Комп'ютерна верстка, макетування В.Ю. Бихун
Дизайн обкладинки О.О. Старовойтенко

Підп. до друку 27.06.2025. Формат 64×90/16.
Папір офсетний. Друк офсетний
Ум. друк. арк. 15,25. Тираж 500 прим. Зам. № 01/7-1

Видавець Бихун В.Ю.
вул. Леонтовича, 9, к. 18, м. Київ, 01054
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції
ДК № 5366 від 26.06.2017 р.
тел./факс: +38 044 235 000 9
моб.: +38 050 310 22 04
e-mail: lk@ukr.net