УДК 342.951

ЦЯПА С.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-9263-1050.

ОГЛЯД ЗАРУБІЖНИХ ЗАКОНОДАВЧИХ ІНІЦІАТИВ СТРАТЕГІЧНОГО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ УМОВАХ

Анотація. *Проаналізовано окремі акти зарубіжного законодавства, присвячені питанням технологічного розвитку штучного інтелекту. Визначено пріоритети та галузі використання штучного інтелекту. Обґрунтовано результативні показники впровадження штучного інтелекту у соціальній сфері, економіці та державному управлінні. Розглянуто ініціативи, які схвалені на державному та міжнаціональному рівнях з метою нормативного врегулювання використання штучного інтелекту у військовій сфері. Окреслені загальносвітові тенденції динамічного розвитку штучного інтелекту в сучасних умовах.*

Ключові слова: *штучний інтелект, цифрові технології, когнітивні технології, нейронні мережі, кібербезпека, кіберзагроза, кібератака, кіберзахист, державна політика, цифровізація, блокчейн, військова сфера.*

Summary. *Some acts of foreign legislation devoted to the issues of technological development of artificial intelligence are analyzed. Priorities and areas of artificial intelligence use have been identified. The effective indicators of introduction of artificial intelligence in the social sphere, economy and public administration are substantiated. The initiatives approved at the state and international levels for the purpose of normative regulation of the use of artificial intelligence in the military sphere are considered. The general world`s tendencies of dynamic development and distribution of technological support of artificial intelligence in modern conditions are outlined.*

Keywords: *artificial intelligence, digital technologies, cognitive technologies, neural networks, cybersecurity, cyberthreat, cyberattack, cyberdefense, state policy, digitalization, blockchain, military sphere.*

Аннотация. *Проанализированы отдельные акты зарубежного законодательства, посвященные вопросам технологического развития искусственного интеллекта. Определены приоритеты и отрасли использования искусственного интеллекта. Обоснованы результативные показатели внедрения искусственного интеллекта в социальной сфере, экономике и государственном управлении. Рассмотрены инициативы, одобренные на государственном и межнациональном уровнях с целью нормативного урегулирования использования искусственного интеллекта в военной сфере. Очерчены общемировые тенденции динамического развития искусственного интеллекта в современных условиях.*

Ключевые слова: *искусственный интеллект, цифровые технологии, когнитивные технологии, нейронные сети, кибербезопасность, киберугроза, кибератака, киберзащита, государственная политика, цифровизация, блокчейн, военная сфера.*

Постановка проблеми. Тотальна епоха цифровізації, розширених технічних та технологічних можливостей кардинально змінює існуючу глобальну соціально-економічну модель світу. Останнім часом технологічне забезпечення штучного інтелекту та його розвиток є сучасним прогресивним напрямком, яким охоплені розвинуті держави світу. Саме когнітивні технології розширюють потенціал інформаційних технологій

з метою вирішення завдань, які традиційно вважалися прерогативою людини та які позбавляють необхідності робити вибір між швидкістю, витратами та якістю. Починаючи з 2017 року, у всесвітніх масштабах розпочалася боротьба за світове лідерство у сфері розвитку штучного інтелекту. З метою унормування подальшого розвитку технологій штучного інтелекту протягом 2017 – 2019 років понад 30 країн світу розробили відповідні національні стратегії (Канада, Сінгапур, КНР, Данія, Італія, Німеччина, Франція), визначивши штучний інтелект одним із важливих пріоритетів державної політики. За таких умов стрімкий розвиток та динамічне використання технологій штучного інтелекту розповсюджується на дедалі більшу кількість сфер та галузей економіки, супроводжуючись значним зростанням як державних, так і приватних інвестицій у їх розвиток. У світових масштабах можна спостерігати навіть конкуренцію між провідними державами у цій сфері. Так, Китай неодноразово заявляв про своє світове лідерство у сфері передових технологій штучного інтелекту вже до 2030 року. У планах офіційного Пекіну прискорені темпи розвитку індустрії штучного інтелекту у сфері проектування та виробництва чипів, у зв'язку з чим влада має намір виділити 16,4 млрд. Євро. Такі самі амбіційні плани у глобальних масштабах останнім часом демонструє і держава-агресор.

На цьому фоні можна констатувати, що провідні країни світу серйозно опікуються цією проблематикою, постійно удосконалюють національне законодавство, присвячене розвитку штучного інтелекту. В умовах цифрових трансформацій кількість як національних інституцій, державних, так і приватних компаній, які тією чи іншою мірою використовують технологічні можливості штучного інтелекту зростає в геометричній прогресії. Практично в сучасних умовах на ринку кібербезпеки вже з'явилися системи з використанням штучного інтелекту. Так, у сфері захисту веб-ресурсів ці системи аналізують середовище та події, які у ньому відбуваються, розпізнають реальні та потенційні загрози, вживають заходів з метою їх усунення та блокування. Інструменти штучного інтелекту оптимізують роботу сайтів, контенту та самостійно налаштовують системи захисту, блокуючи при цьому шкідливий трафік та забезпечуючи надходження безпечного контенту. Адже застосування штучного інтелекту не обмежується виключно захистом веб-ресурсів. Ще однією поширеною сферою його застосування є суттєве зменшення уразливостей та ризиків в системах забезпечення кібербезпеки. Адже не можна недооцінювати роль та значення технологій штучного інтелекту, особливо в умовах транснаціонального розповсюдження гібридних загроз, кібератак, глобального поширення пандемії, коли тренд переходу на віддалений режим роботи задає високу планку та нові вимоги до сучасних систем безпеки.

В сучасних умовах Україна робить лише перші поступальні кроки з метою нормативного забезпечення процесів розробки та впровадження технологій штучного інтелекту у загальну концепцію побудови безпеки цифрових сервісів та електронних послуг. Тому висвітлення проблемних питань використання штучного інтелекту у сфері забезпечення кібербезпеки, визначення подальших шляхів удосконалення законодавчих основ у цій площині є актуальним та своєчасним, особливо враховуючи проголошений курс України на тотальну цифровізацію усіх сфер суспільного життя у рамках реалізації з 2019 року амбіційного проекту "Держава у смартфоні".

Результати аналізу наукових публікацій. Технології штучного інтелекту та їх вплив на стан забезпечення кібербезпеки певною мірою досліджували у своїх працях такі науковці: В. Брижко [1], О. Бусол [2], О. Радутний [3], В. Савченко [4], тощо. Питання правового врегулювання засад розвитку штучного інтелекту розглядали: О. Баранов [5], А. Бежевець [6], О. Косілова [7], О. Кривецький [8], К. Міліцина [9] та ін.

Проте вбачаються недостатньо висвітленими сучасні зарубіжні законодавчі ініціативи, які останнім часом впроваджуються з метою правового врегулювання сфери застосування технологій штучного інтелекту, що посилює актуальність цієї роботи.

Метою статті є оцінка нормативно-правових актів окремих держав світу та узагальнення стратегічних напрямів розбудови вітчизняної екосистеми інноваційних розробок у сфері технологій штучного інтелекту.

Виклад основного матеріалу. Світовою спільнотою було розроблено такий показник, як "Індекс готовності урядів до впровадження штучного інтелекту" (Government Artificial Intelligence Readiness Index) [10]. Так, у 2020 році Україна посіла 57-е місце у цьому загальносвітовому рейтингу держав світу, країна – агресор (РФ) 33-е місце, а Білорусь – 66. На цьому фоні, наша держава також розвиває власне законодавство та формує концептуальні засади державної політики в галузі штучного інтелекту, наближаючи його до кращих практик міжнародного досвіду, переслідуючи мету створення конкурентоспроможного середовища у соціально-економічній, науково-технічній, оборонній та інших сферах життєдіяльності. За таких умов, у вітчизняних реаліях технології штучного інтелекту повинні сприяти прискоренню трансформації економіки, ринку праці, державних інституцій та суспільства в цілому.

З метою проведення порівняльно-правового аналізу, розглянемо концептуальні засади регулювання технологій штучного інтелекту в Республіці Білорусь. Так, Концепція інформаційної безпеки, яка затверджена Постановою Ради Міністрів Республіки Білорусь 18 березня 2019 року [11], нормативно регламентує прагнення політичного керівництва цієї країни прискорити запровадження цифрової трансформації економіки як важливої складової формування інформаційного суспільства, що має призвести до того, що усі галузі, ринки, сфери життєдіяльності держави мають бути переорієнтовані на нові цифрові економічні моделі. Зазначається, що в Білорусі активно розвиваються інноваційні цифрові технології, засновані на системах штучного інтелекту, нейронних мереж, що забезпечують роботу з численними інформаційними ресурсами, у тому числі й масивами Великих даних, технології реєстру блоків трансакцій (блокчейн). При цьому акцентовано, що у цій країні ступінь цифровізації галузей економіки є диференційованою, що значно знижує очікуваний синергічний ефект від запровадження синхронної інформатизації, у зв'язку з чим цифрова політика держави має орієнтуватися на реалізацію пілотних проектів цифровізації та їх галузеве масштабування, створення центрів компетенції з питань цифрової трансформації. Задекларовано, що у якості найбільш вірогідних джерел загроз кібербезпеки виступають: збої технічних засобів та програмного забезпечення в інформаційних та телекомунікаційних системах, протиправна діяльність окремих осіб та злочинних угрупувань, помилки персоналу інформаційних систем, які проявляються у порушенні встановлених регламентів їх експлуатації та правил обробки інформації, залежність Білорусі від інших держав – виробників програмних та апаратних засобів при створенні та розвитку інформаційної інфраструктури. Кібербезпека національного сегменту мережі Інтернет забезпечується переважно за рахунок відбиття основного обсягу кібератак на інформаційні системи та мережі передачі даних шляхом блокування шкідливих комунікацій між суб'єктами та об'єктами впливу. Тобто, "людський фактор" залишається, у тому числі, однією із актуальних загроз кібербезпеці держави, що диктує необхідність використання технологій штучного інтелекту з метою нівелювання цієї загрози.

Постановою Ради Міністрів Республіки Білорусь від 2 лютого 2021 року № 66 була затверджена Державна програма "Цифровий розвиток Білорусі на 2021 – 2025 роки" [12]. Цим програмним документом проголошено курс на прискорення впровадження

цифрових інновацій та технологій “розумних міст”, забезпечення інформаційної безпеки таких рішень. Передбачається виконання заходів щодо створення сучасної інформаційно-комунікаційної інфраструктури та комплексної цифрової трансформації процесів державного управління, регіонального та галузевого розвитку, у тому числі й у таких сферах як: охорона здоров’я, освіта, екологічна безпека, стабільний розвиток населених пунктів тощо.

Також визначено засади та перелік заходів, реалізація яких надасть змогу впровадити у реалії життя передові інформаційні технології, прискорити інтеграцію економіки Білорусі у світовий економічний цифровий простір. При цьому достатня увага приділяється штучному інтелекту в контексті розв’язання сучасних цифрових рішень й завдань. Розвиток інформаційних технологій, заснованих на впровадженні технічних рішень, державних електронних сервісів, має призвести до необхідності безперервного удосконалення інструментів, які мають забезпечувати стабільність їх роботи та захист даних державних інформаційних систем (цифрових платформ).

Очікується, що практична реалізація положень цієї Державної програми дозволить: підвищити рівень інформаційної безпеки даних та технологій її забезпечення у рамках створення розгалуженої цифрової інформаційної екосистеми; забезпечити конкурентоздатність вітчизняних розробок та технологій інформаційної безпеки; створити ефективну систему захисту прав та законних інтересів громадян, бізнесу та держави від загроз інформаційної безпеки. Ключовим завданням впровадження технологій штучного інтелекту у сфері забезпечення інформаційної безпеки має стати зміцнення довіри громадян, забезпечення умов для безпечного надання та отримання електронних послуг, включаючи розробку програмних та програмно-апаратних комплексів захисту інформаційних ресурсів, інформаційно-телекомунікаційних систем, формування та удосконалення технічних умов з метою надійної ідентифікації в рамках надання державних послуг та здійснення адміністративних процедур в електронній формі.

Узагальнюючи вищевикладене, можна констатувати, що в Білорусі під штучним інтелектом розуміють глибокі штучні нейронні мережі та технологію на їх основі, які дозволяють вирішувати складні завдання обробки масивів інформації. Технології штучного інтелекту покликані імітувати когнітивні функції людського інтелекту, що дозволяє системі здійснювати обробку та інтерпретувати інформацію, аналізувати її та робити висновки, використовуючи й адаптуючи ці знання для досягнення мети, з якою ця технологія була впроваджена. Застосовуючи штучний інтелект та алгоритми глибокого навчання у сфері кібербезпеки, можливо виграти час, що є критичним елементом у будь-якій ситуації під час поширення кібератак. Для Білорусі штучний інтелект виступає революційною технологією у сфері забезпечення кібербезпеки, при цьому саме технології машинного навчання та комп’ютерного зору відкривають нові перспективи для розвитку сучасних засобів захисту інформації. Типовими формами його практичної реалізації є розробка та впровадження відповідних пілотних проектів. Наприклад, в Мінському обласному управлінні Департаменту охорони МВС Республіки Білорусь у січні 2020 року стартував пілотний проект моніторингу безпеки території за допомогою штучного інтелекту. При цьому у якості основи інфраструктури системи комплексної безпеки були обрані інтелектуальні модулі, засновані на нейронних мережах.

Держава-агресор (РФ) з метою реалізації своїх імперських задумів та проведення наступальних операцій, у першу чергу, в кіберпросторі, особливо проти України, ще у жовтні 2019 року схвалила Національну стратегію розвитку штучного інтелекту до 2030 року [13]. Невипадково нормативно задекларовано амбіційне прагнення РФ посісти

міжнародні лідерські позиції у сфері розвитку та використання технологій штучного інтелекту у всіх сферах життєдіяльності, включаючи такі сегменти як оборона та безпека.

Цікавим видається досвід Узбекистану у цій площині, країни, де першочерговим пріоритетом визначено штучний інтелект та технології його впровадження. У зв'язку з цим Президент цієї країни 17 лютого 2021 року підписав Постанову "Про заходи щодо створення умов для прискорення впровадження технологій штучного інтелекту" [14]. Цим документом заплановано розробку Національної стратегії розвитку штучного інтелекту, яка передбачатиме підготовку цільової державної програми підтримки наукових досліджень та інноваційних проектів у сфері штучного інтелекту, "дорожню карту" реалізації положень Стратегії, цільові показники (індикатори) розвитку цієї сфери; підвищення доступності та якості цифрових даних, розробку програмних продуктів; створення сучасної високотехнологічної інфраструктури та апаратних комплексів для вирішення завдань у сфері штучного інтелекту; організацію підготовки кваліфікованих спеціалістів у цій сфері, в тому числі й із залученням зарубіжних викладачів, цільового навчання кадрів для пріоритетних галузей економіки, соціальної сфери, системи державного управління; розробку комплексної системи регулювання питань впровадження та застосування технологій штучного інтелекту, загальних керівних принципів та норм, а також єдиних стандартів й правил обробки цифрових даних; удосконалення системи контролю та запобігання ризикам у сфері штучного інтелекту, у тому числі забезпечення безпечного функціонування програм, розроблених на основі технологій штучного інтелекту, а також профілактики потенційних ризиків, а також конфіденційності використаних даних. Також передбачається схвалення на національному рівні міжнародних стандартів у сфері штучного інтелекту, створення та запровадження спеціального правового режиму щодо застосування технологій штучного інтелекту.

Стратегічним напрямком визначена розбудова вітчизняної екосистеми інноваційних розробок у сфері штучного інтелекту, що передбачатиме: утворення науково-дослідного інституту розвитку цифрових технологій та штучного інтелекту, запровадження механізмів спільного фінансування (краудфандингу) у стартап-проєктах у сфері штучного інтелекту, проведення відкритих занять у закладах освіти. Достатня увага також приділяється питанням: формування інвестиційної привабливості та здійснення розробок у сфері штучного інтелекту; забезпечення доступу вітчизняних підприємств та спеціалістів до інформаційних ресурсів у сфері штучного інтелекту, налагодження плідного міжнародного співробітництва у сфері штучного інтелекту та технологій його застосування. Нормативно заплановано впровадження технологій у сфері штучного інтелекту в Узбекистані протягом 2021 – 2022 років у таких галузях: сільське господарство, банківський сектор, фінанси, транспорт, охорона здоров'я, електронне урядування. Загальний обсяг фінансування, закладений з метою виконання цих програм, складає 200 млрд. Сумів.

Нормативно задекларовано, що з метою стимулювання залучення інвестицій у технологічне оснащення штучного інтелекту повинні бути розроблені інструменти державно-приватного партнерства, запроваджені фінансові та податкові пільги для розробників та інвесторів, включаючи венчурне фінансування. Для побудови ефективних рішень на базі штучного інтелекту у таких сферах як безпека, освіта, охорона здоров'я потребується запровадження єдиної системи збору та аналізу даних з уніфікованим доступом та суцільною деперсоналізацією. Таким чином, Узбекистан, адаптуючи кращі практики зарубіжного досвіду, розробив та впроваджує власну модель технологічного забезпечення штучного інтелекту цивільного сектору, активно опікується питаннями розробки власної нормативно-правової бази, яка визначатиме

єдині критерії та вимоги, засади відповідальності й безпечності під час розробки та використання технологій штучного інтелекту в провідних галузях економіки та соціальній сфері, системі державного управління.

Україна також не стоїть осторонь процесів удосконалення правового регулювання технологій штучного інтелекту та виражає прагнення зайняти значний сегмент світового ринку технологій штучного інтелекту, провідні позиції у міжнародних рейтингах. Зокрема, у грудні 2020 року в Україні була схвалена Концепція розвитку штучного інтелекту [15], практична реалізація якої сприятиме інтеграції інноваційних технологій в економічно важливі сектори держави. Очікується, що технології штучного інтелекту сприятимуть трансформації економіки, ринку праці, державних інституцій та суспільства загалом. Їх застосування надасть можливість зменшити обсяги витрат і підвищити ефективність виробництва, якість товарів та послуг. Метою цієї Концепції є визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб, побудови конкурентоспроможної національної економіки, вдосконалення системи публічного управління. Пріоритетними сферами, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, нормативно визначені: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя. Згідно із положеннями чинного законодавства штучний інтелект – організована сукупність інформаційних технологій, із застосуванням яких можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань.

Особлива увага у її положеннях присвячена розвитку штучного інтелекту саме у сфері кібербезпеки. Чинним законодавством України встановлено, що основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об’єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян. Комплексне розв’язання проблем кібербезпеки у цьому форматі вимагає виконання таких завдань: удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту; розроблення інноваційних систем кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчення питання ліцензування іноземних розробок штучного інтелекту у сфері кібербезпеки, особливо у державному секторі; створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління; оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей Хмарних обчислень. Оновлення стандартів та розроблення нових необхідно здійснювати з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032.

Загалом можна констатувати, що у питаннях розроблення стандартів у сферах новітніх технологій, зокрема штучного інтелекту, наша держава виходить з того, що всесвітня глобальна мережа має залишатися глобальною та відкритою, технології повинні орієнтуватися на людину, забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині повинні здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним. Водночас, у зв'язку з ускладненням міжнародної безпеки в кіберпросторі Україна займає більш проактивну позицію в дискусіях ООН та інших міжнародних форумах для просування, координації та консолідації її позиції у сфері забезпечення кібербезпеки, зменшуючи актуальні небезпеки мілітаризації кіберпростору. За таких умов, одним із ключових завдань для держави залишається прискорення впровадження технологій штучного інтелекту в національній системі кібербезпеки, посилення спроможностей її відповідальних суб'єктів.

Розглянемо деякі ініціативи, які схвалюються як на державному, так і міжнаціональному рівнях з метою нормативного врегулювання використання штучного інтелекту саме у військовій сфері. Так, розуміючи актуалізацію сучасних тенденцій поширення технологій штучного інтелекту у світових масштабах, на початку 2020 року Пентагон схвалив етичні принципи для впровадження штучного інтелекту в свою діяльність. Успіхи РФ та КНР у військовій сфері, прискорений розвиток сучасних оборонних технологій сприймаються в американському оборонному відомстві як серйозний і потужний виклик, що провокує активізацію розробок у сфері високих технологій з використанням нейтронних мереж. Невипадково, у цих принципах закладено базові основи етичного проектування, розробки та використання штучного інтелекту міністерством оборони США.

Слід вказати, що нові технології, такі як штучний інтелект, автономні та квантові технології змінюють характер діяльності НАТО. Розуміючи ризики та можливості, які несуть нові технології Північноатлантичному Альянсу, міністри оборони держав-членів НАТО на щорічному саміті у лютому 2021 року схвалили стратегію впровадження нових та революційних технологій. Загальна мета цього програмного документа – розробка власної інноваційної системи комплексної взаємодії в рамках Альянсу, яка надасть змогу використовувати тотожні підходи та однакові технології для усіх учасників блоку. Для загального управління цим процесом запропоновано створити власну інституцію (агентство), а з метою здійснення фінансування – інвестиційний банк НАТО з венчурним фондом, який буде функціонувати за рахунок внесків держав-членів, забезпечуючи надання субсидій та грантів на перспективні проекти. Очікується, що влітку 2021 року НАТО схвалить власну стратегію, присвячену питанням розвитку сфери технологій штучного інтелекту та обробки даних, оскільки цей напрямок є і залишається загальною частиною загальної стратегії інвестицій НАТО в нові та революційні технології. Ця стратегія визначатиме шляхи заохочення та захисту розробок у сфері штучного інтелекту та його технологій з метою збереження технологічного домінування НАТО у глобальній військовій сфері, буде містити плани стандартизації взаємодії та розвитку технологій, включати рекомендації відповідального використання платформ з підтримкою штучного інтелекту. Запланована плідна співпраця НАТО з партнерами, науковими установами, приватним сектором, включаючи стартапи з метою зміцнення економічного потенціалу та промислової бази союзників.

У рамках реалізації повістки "НАТО – 2030" важливе місце також посідають оборонні інновації, спрямовані на покращення трансатлантичного співробітництва у сфері впровадження та розвитку критично важливих технологій. Тобто кінцевою метою є прагнення Альянсу зберегти технологічне домінування та перемогти Китай, Росію та інших великих гравців під час гонки технологічного озброєння. У фокусі уваги НАТО сконцентровані такі питання як: створення оперативної мережі інноваційних центрів, просування успішних інноваційних бізнес-моделей та оперативних моделей, підвищення спроможностей й рівня технічної та цифрової грамотності персоналу.

Висновки.

Роль та значення технологій штучного інтелекту у світових масштабах не можна недооцінювати. В сучасних умовах у світі відбувається прискорення впровадження технологічних рішень, розроблених на основі штучного інтелекту у різних галузях економіки, державного управління та сферах суспільних відносин. Практичне використання технологій штучного інтелекту передбачає обробку великих масивів даних та машинне навчання, за якого програми та алгоритми постійно удосконалюються. Штучний інтелект дозволяє практично повністю виключити людський фактор з процесів забезпечення захисту інформації та залишає лише допоміжні функції моніторингу та корекції. У зв'язку з цим штучний інтелект є технологією майбутнього. За оцінками експертів, очікується, що завдяки впровадженню таких рішень зростання світової економіки у 2024 році дорівнюватиме $1 трлн. Штучний інтелект та його технології відкривають нові горизонти в епоху цифровізації та розпочинають активно використовуються у цивільній та військовій сферах.

Кожна держава світу, розуміючи переваги штучного інтелекту намагається законодавчо врегулювати сфери його використання. Аналіз висвітлених нормативно-правових актів дає змогу визначити форми впровадження технологій штучного інтелекту у тій чи іншій країні світу, якими виступають: розробка та реалізація пілотних проектів, запровадження фінансових та податкових пільг для розробників та інвесторів, затвердження керівних принципів та етнічних норм використання штучного інтелекту тощо. Ключовим питанням для країн світу залишається формат фінансування відповідних розробок та обсяг залучених інвестицій для розвитку технологій штучного інтелекту.

Як не парадоксально, навіть країни третього світу із значним технологічним відставанням, на кшталт Узбекистану, переймаються проблемою актуалізації прискорення впровадження технологій штучного інтелекту у реалії повсякденного життя. За таких умов у світі спостерігається активізація та динамічний розвиток цієї сфери, а для деяких країн світу вимальовуються перспективи нарощування потужностей з метою протистояння та боротьби за глобальне технологічне домінування. Також чином, можливо підсумувати, що саме технології штучного інтелекту беззаперечно є рушійною силою у питаннях забезпечення безпеки та оборони, про що яскраво свідчать останні кроки та ініціативи, які здійснюють Пентагон та НАТО. Світ поступово переходить у нову еру протистояння та реагування на виклики й загрози за допомогою штучного інтелекту, у тому числі й у військових конфліктах, про що свідчить започаткована гонка технологічних озброєнь між провідними країнами світу (США, КНР, РФ) з метою встановлення й опанування світового цифрового лідерства.

Використана література

1. Брижко В.М., Фурашев В.Н. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право*. № 1(20)/2017. С. 51-67.

2. Бусол О.Ю. Потенційна небезпека штучного інтелекту. *Інформація і право*. № 2(14)/2015. С. 121-127.

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

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

5. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5-6. С. 75-95.

6. Бежевець А.М. Правовий статус роботів: проблеми та перспективи визначення. *Інформація і право*. № 1(28)/2019. С. 61-67.

7. Косілова О.І., Солодовнікова Х.К. Права і свободи людини і громадянина v.s. штучний інтелект: проблемні аспекти. *Інформація і право*. № 4(35)/2020. С. 56-66.

8. Кривецький О. До проблеми правового регулювання штучного інтелекту. *Громадська думка про правотворення*. 2018. № 14. С. 15-19. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=3728:do-problemi-pravovogoregulyuvannya-shtuchnogo-intelektu&catid=8 &Itemid=350

9. Міліцина К. Об'єкти, створені за допомогою штучного інтелекту і штучним інтелектом безпосередньо, та авторське право США. *Підприємництво, господарство і право*. 2019. № 5. С. 343-346.

10. Government Artificial Intelligence Readiness Index 2020. URL: https://www.oxfordinsights.com/government-ai-readiness-index-2020 (дата звернення: 20.02.2021).

11. О Концепции информационной безопасности Республики Беларусь: Постановление Совета Министров Республики Беларусь от 18 марта 2019 года № 1. URL: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf (дата звернення: 20.02.2021).

12. О государственной программе "Цифровое развитие Беларуси" на 2021 – 2025 годы: Постановление Совета Министров Республики Беларусь от 2 февраля 2021 года № 66. URL: https://pravo.by/document/?guid=12551&p0=C22100066&p1=1&p5=0

13. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 года № 490. URL: https://www.garant.ru/products/ipo/prime/doc/72738946/#1000 (дата звернення: 20.02.2021).

14. О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта: Постановление Президента Республики Узбекистан от 17 февраля 2021 года № 4996. URL: https://lex.uz/docs/5297051(дата звернення: 20.02.2021).

15. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 20.02.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~