УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор*, ГО «Міжнародна академія інформації», професор НА СБ України
ORCID: https://orcid.org/0000-0003-0069-3727

ПЕТРОВ С.Г., *доктор юридичних наук*, провідний науковий співробітник, Інституту спецзв'язку та захисту інформації НТУ України «Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: https://orcid.org/0000-0001-7786-4657

ТЕНДЕНЦІЇ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАРУБІЖНИХ КРАЇНАХ

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346350

Анотація. *У статті здійснено аналіз тенденцій розвитку правового регулювання штучного інтелекту у зарубіжних країнах. Доведено, що на сьогодні відсутні міжнародно-правові імперативні нормативи у сфері ШІ. Правове регулювання ШІ у США послабилося після скасування Указу №14110 про безпечну, захищену та надійну розробку та використання ШІ. Не достатньо регульоване використання ШІ як у новітніх продуктах великих ІТ компаній, так і у державних структурах США є загрозою порушення прав людини і навіть національних інтересів інших держав.*

Китай також призупинив розробку проекту Закону "Про штучний інтелект". Проблеми конфіденційності та безпеки даних ШІ DeepSeek, розробленої у Китаї, спричинили заборону цього продукту в кількох країнах і державних установах через загрози національній безпеці, зокрема через потенційний доступ китайського уряду до даних, що збирає DeepSeek.

У Китаї існує значний державний контроль за сферою генеративних послуг штучного інтелекту, зокрема послуг "глибоких фейків" ("deep fake") з вимогами для провайдерів обов'язкового інформування Міністерства громадської безпеки Китаю.

Зроблено висновок, що законодавство ЄС щодо штучного інтелекту містить механізми захисту прав людини від імовірного негативного впливу внаслідок розробки і використання систем штучного інтелекту. Закон ЄС про штучний інтелект та інфраструктура нагляду, що наразі формується у Євросоюзі, є гарантією дотримання прав людини у цій чутливій сфері.

Ключові слова*: інформаційне право, законодавство, штучний інтелект, правове регулювання, національна безпека.*

Summary. *The article analyzes the trends in the development of legal regulation of artificial intelligence in foreign countries. It is proven that there are currently no international legal imperative standards in the field of AI. Legal regulation of AI in the USA has weakened after the repeal of Decree No. 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The insufficiently regulated use of AI in both the latest products of large IT companies and in US government structures poses a threat to human rights.*

China has also suspended the development of a draft Law "On Artificial Intelligence". Problems with the confidentiality and data security of the DeepSeek AI, developed in China, have led to the banning of this product in several countries and government agencies due to threats to national security, in particular due to the potential access of the Chinese government to the data collected by DeepSeek.

In China, there is a significant state control over the area of generative AI services, including "deep fake" services, with providers required to report to the Chinese Ministry of Public Security.

It is concluded that EU legislation on artificial intelligence contains mechanisms to protect human rights from potential adverse impacts resulting from the development and use of artificial intelligence systems. The EU Law on Artificial Intelligence and oversight infrastructure, currently being developed in the European Union, is a guarantee of human rights in a sensitive area of AI.

***Keywords**: Information Law, Legislation, Artificial Intelligence, Legal Regulation, National Security.*

Постановка проблеми.

Інформаційне право зарубіжних країн продовжує розвиватися із розвитком міжнародно-правового регулювання у сфері штучного інтелекту (далі – ШІ). До концептуальних і рекомендаційних документів на кшталт Рекомендацій ЮНЕСКО щодо етики ШІ, принципів ОЕСР щодо ШІ, документів Хіросімського процесу, Сеульської декларації, Декларація Блетчлі, Глобального цифрового договору ООН та інших, запроваджених ООН чи іншими організаціями, додаються рішення національних урядів, насамперед США і ЄС, які значно впливають на подальше нормотворення у сфері розробки і використання ШІ.

Однак відсутність огляду тенденцій розвитку правового регулювання ШІ у зарубіжних країнах, вимагає аналізу теоретичних основ і практики розвитку правових механізмів у США, ЄС і Китаї. Однією з проблем генеративного ШІ є так звана проблема "чорного ящика", коли не завжди можливо повністю зрозуміти, як працює технологія або на якій основі генерується відповідь. Тому цьому питанню розвитку суспільних відносин і їх правового регулювання щодо генеративного ШІ, а також використанню ШІ у сферах безпеки і оборони приділено особливу увагу у цій статті.

Аналіз останніх досліджень і публікацій свідчать про те, що подібні питання регулювання нових інформаційних технологій, зокрема ШІ були частково предметом досліджень українських учених, а саме Волкова Ю.Ф., Пирога І.С. [1], Попова Н.О [2], Макух-Федоркова, І., Мікіцел, Д. [3], Котуха О.С., Попов Д.І. [4].

Зарубіжними вченими досліджуються проблеми регулювання систем ШІ та пропонується адаптована модель регулювання, що підходить для нових функцій ШІ [5], особливості закону Європейського Союзу про ШІ [6], визначення предмету правового регулювання відносин щодо ШІ [7] тощо. Автори цієї статті також частково розглядали питання протидії дезінформації на основі ШІ за допомогою національного регулювання [8].

Однак у цілому питання розкриття тенденцій розвитку правового регулювання ШІ у зарубіжних країнах було предметом наукових досліджень лише фрагментарно.

Метою статті є розкриття тенденцій розвитку правового регулювання ШІ у зарубіжних країнах.

Виклад основного матеріалу.

Людство є свідком глобальної гонки озброєнь у сфері ШІ, основними суб'єктами якої є США і Китай. Зокрема, у документах з національної безпеки цих та інших держав ШІ визначається як критично важливий для підтримки військової переваги. Вже не потенційними, а реальними загрозами національній безпеці України зокрема є використання систем ШІ для створення профілів осіб для протиправних цілей, для здійснення кібератак проти критичної інфраструктури, під час ведення бойових дій російською федерацією тощо. Саме тому доцільно звернути увагу на міжнародно-правові передумови для розвитку національного регулювання ШІ у зарубіжних державах.

Структури ООН намагаються створити платформи і міжнародно-правові механізми для визначення принципів регулювання відносин щодо ШІ. Так, Глобальний цифровий договір, Панель та діалог щодо ШІ [9] передбачають доволі прогресивні ініціативи як створення в рамках ООН міждисциплінарної незалежної міжнародної наукової групи з питань ШІ та ініціювання діалогу щодо управління ШІ за участю урядів, а також розробку інноваційних варіантів добровільного фінансування розвитку потенціалу ШІ. Однак до створення Конвенції чи іншого загальнообов'язкового міжнародного документу, на нашу думку, пройде ще не один рік.

Документи та дослідження ООН щодо ШІ мають переважно рекомендаційний характер. Оскільки ШІ за своєю природою має міжгалузевий характер застосування, то і до проблем регулювання або управління ШІ на рівні ООН спостерігається фрагментарний підхід. До прикладу, дослідження міжнародних принципів використання ШІ в судових системах буде оприлюднено на 80-й сесії Генеральної Асамблеї ООН у жовтні 2025 року. Незалежний доповідач Маргарет Саттертуейт включить до звіту інформацію щодо того, як ШІ використовується суддями, зокрема при винесенні рішень, яке навчання з використанням ШІ доступне для суддів, хто його розробляє, організовує та фінансує, які інструменти ШІ створюються та інтегруються в судову систему. Розглядатимуться також юридичні консультації чат-ботів, а також можливості юридичного представництва на основі ШІ та вирішення спорів онлайн за допомогою ШІ [10].

Таким чином, за відсутності міжнародно-правових імперативних нормативів у сфері ШІ, які, насамперед, були б спрямовані на захист прав людини від потенційних загроз, необхідно зосередити увагу на тенденціях правового регулювання у США, Китаї та ЄС.

У США система правового регулювання ШІ значно послабилася у 2025 році. Фактично було скасовано норми Указу Президента Байдена №14110 про безпечну, захищену та надійну розробку та використання ШІ [11], відповідно усі інші документи, шо були прийняті на виконання цього Указу, стали нелегітимними, зокрема Рамкова основа для вдосконалення управління ШІ і управління ризиками в національній безпеці [12], розроблена Національним інститутом стандартів і технологій (NIST) США.

Штучний інтелект (ШІ) має потенціал трансформувати як бойові дії, так і операції допоміжного управління Міністерством оборони США. Сполучені Штати повинні активно впроваджувати ШІ у своїх Збройних силах, якщо вони хочуть зберегти свою глобальну військову перевагу, а також забезпечити, як зазначено в цьому Плані дій, безпечне та надійне використання ШІ. Оскільки Міністерство оборони США має унікальні операційні потреби в рамках федерального уряду, воно заслуговує на конкретні політичні дії для стимулювання впровадження ШІ.

План дій США щодо ШІ [13], оприлюднений у липні 2025 року, передбачає зокрема захист комерційних та урядових інновацій у сфері ШІ. Державні органи США мають співпрацювати із провідними американськими розробниками ШІ, щоб приватний сектор міг активно захищати інновації ШІ від ризиків безпеки, включаючи зловмисних кіберсуб'єктів, внутрішні загрози та інші.

Хоча проекти, пов'язані зі ШІ продовжуються як на рівні великих ІТ компаній, так і у державних структурах. Зокрема, Спільний центр ШІ (JAIC), створений у 2018 році для координації зусиль у сфері ШІ та розробки застосувань для військового використання, продовжує свою активну діяльність із впровадження передових комерційних технології ШІ у Міністерстві оборони США, із певними організаційними трансформаціями [14]. Продовжує свою діяльність у сфері ШІ також Агентство

передових оборонних дослідницьких проектів (DARPA), яке керує кількома програмами на основі ШІ. Зокрема, у серпні 2025 року система кіберреагування, розроблена командою Atlanta, продемонструвала здатність нових автономних систем, що використовують ШІ, захищати програмне забезпечення з відкритим кодом, яке лежить в основі критичної інфраструктури [15]. Крім того, приклади зброї з підтримкою ШІ включають безпілотник MQ-9 Reapr, який використовує ШІ для ідентифікації та відстеження цілей, і Sea Hunter, автономне військово-морське судно, призначене для боротьби з підводними човнами [16].

Зазначені приклади свідчать, що відносини, пов'язані із розробкою і використанням ШІ інтенсивно розвиваються у США. Однак після скасування Указу Президента Байдена №14110 про безпечну, захищену та надійну розробку та використання ШІ, викликає занепокоєння фактично неконтрольоване і необмежене використання ШІ як у новітніх продуктах великих ІТ компаній, так і у державних структурах США.

Звернемо увагу на розвиток відносин, пов'язаних із ШІ, а також відповідного правового регулювання в Китаї.

У "Плані розвитку штучного інтелекту наступного покоління" Китаю 2017 року ШІ визначено як стратегічний пріоритет і центр глобальної конкуренції [17]. Досягнення в обробці мови та розпізнаванні облич підтримують амбіції Китаю щодо домінування у сфері ШІ, зокрема завдяки інтеграції з внутрішнім спостереженням. Китай також розробляє автономні військові транспортні засоби та технологію рою для подолання протиракетної оборони.

Великі ІТ компанії цієї країни у 2025 році створили конкурентні ШІ системи, наприклад китайський стартап ШІ DeepSeek, який був випущений Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. (Китай) на противагу ChatGPT та іншим великим мовним моделям (LLM). Deep Seek AI прагне розширити межі ШІ для створення рішень, які покращують людські можливості, зробити передові технології ШІ доступними та ефективними [18].

Варто відзначити, що через проблеми конфіденційності та безпеки даних ШІ DeepSeek вже заборонено в кількох країнах і державних установах, зокрема через потенційний доступ китайського уряду до даних, що збирає DeepSeek. Австралія, Тайвань, Нідерланди, Японія, Канада, Італія, Південна Корея та США вже обмежили або заборони використання ШІ DeepSeek загалом в країні або для державних службовців [19].

Стосовно правового регулювання відносин, пов'язаних із ШІ, заначимо, що Китай призупинив розробку проекту Закону "Про штучний інтелект" через розбіжності між промисловістю і науковцями. Тим часом діють Положення про управління алгоритмічними рекомендаціями інформаційних послуг Інтернету та Адміністративні положення про управління глибоким синтезом інформаційних послуг Інтернету [20].

25 квітня 2025 року Державне управління з регулювання ринку та Управління стандартизації Китаю спільно опублікували три національні стандарти, спрямовані на підвищення безпеки та управління генеративним ШІ. Ці стандарти офіційно набудуть чинності 1 листопада 2025 року і визначають вимоги безпеки для процесів маркування даних, що використовуються в навчанні моделей ШІ [21], окреслюють вимоги та критерії оцінки для забезпечення безпеки наборів даних, що використовуються на етапах попереднього навчання та точного налаштування розробки генеративного ШІ [22], а також вимоги безпеки для генеративних сервісів ШІ, що охоплюють оцінку

безпеки даних користувачів, заходи захисту даних та захист моделей навчання та наборів даних [23].

Китай на сьогодні вважається головним конкурентом США у світовій індустрії ШІ. І хоча дані про конкретні проекти Китаю щодо "оборонного" ШІ важко отримати через обмежену публічну прозорість, Народно-визвольна армія значно інвестує в ШІ.

Здійснений аналіз законодавства Китаю дає підстави для висновку, що аналогічно із іншими сферами, у цій державі передбачається значний державний контроль за сферою генеративних послуг ШІ, зокрема послуг "глибоких фейків" ("deep fake"). Зокрема, постачальники послуг зобов'язані співпрацювати з регуляторними органами з нагляду та інспекції, постачальники, які пропонують послуги "глибокого синтезу" ("глибоких фейків", "deep fake"), повинні маркувати будь-які візуальні матеріали чи відео, щоб попередити громадськість про їхню природу. Якщо будь-яка послуга має ознаки впливу на громадську думку або має здатність до "соціальної мобілізації", постачальник послуг повинен провести оцінку безпеки, яка повинна бути подана до місцевих відділень Міністерства громадської безпеки Китаю.

Найбільш структурованим є законодавство ЄС щодо ШІ. У ньому відображено механізми врахування і захисту прав людини від імовірного негативного впливу внаслідок розробки і використання систем ШІ. Положення Закону ЄС про штучний інтелект [24] поступово набирають чинності, розвиваються структури управління Європейська рада зі Ш вже функціонує, а наукова група незалежних експертів та консультативний форум Закону про ШІ перебуває у процесі формування. Активно розвивається підзаконне нормативно-правове регулювання в ЄС, наприклад, опублікований 9 квітня 2025 року План дій континенту щодо ШІ [25], свідчить також про долучення ЄС до боротьби США і Китаю за домінування у сфері ШІ.

План дій континенту щодо ШІ передбачає створення 13 фабрик ШІ по всій Європі за допомогою провідної суперкомп'ютерної мережі. Ці фабрики підтримуватимуть стартапи, промисловість і дослідників у розробці передових моделей і додатків ШІ. Планується створення до 5 гігафабрик ШІ, великомасштабних об'єктів із величезною обчислювальною потужністю та центрів обробки даних для тренувань складних моделей ШІ в надвеликому масштабі.

План дій континенту щодо ШІ передбачає потроєння потужностей центрів обробки даних ЄС протягом наступних 5-7 років, віддаючи пріоритет стійким центрам обробки даних. Планується також розробити стратегію об'єднання даних для створення внутрішнього ринку даних, а також лабораторії даних на фабриках ШІ для збору та організації високоякісних даних із різноманітних джерел. ЄС планує просувати ШІ в промисловість, державний сектор і охорону здоров'я, будуть відкриті шляхи легальної міграції для висококваліфікованих працівників у галузі ШІ з країн, що не входять до ЄС, запускатимуться освітні та навчальні програми з ШІ та генеративного ШІ в ключових секторах економіки. ЄС також впроваджує ініціативу InvestAI, яка мобілізує 200 мільярдів євро для інвестицій у ШІ в Євросоюзі.

На сьогодні постачальники послуг, пов'язаних із ШІ, мають можливість добровільно дотримуватися вимог Кодексу практики щодо ШІ загального призначення [26].

Моделі ШІ загального призначення навчаються на великих обсягах даних, але доступна лише обмежена інформація щодо походження цих даних. У розвиток положень Закону ЄС про ШІ 2 серпня 2025 року набули чинності зобов'язання (шаблон) щодо моделей ШІ загального призначення [27]. Зобов'язання (шаблон) надає вичерпний огляд даних, використаних для навчання моделі, перелік основних колекцій даних та

пояснення інших використаних джерел, а також допоможе сторонам із законними інтересами, таким як власники авторських прав, у здійсненні своїх прав згідно із законодавством ЄС.

ЄС також звертає увагу на використання ШІ у сфері безпеки та оборони [16]. Оборонні інновації на основі ШІ в ЄС переважно реалізуються через проекти Європейського оборонного фонду [28] та постійного структурованого співробітництва [29].

Держави-члени ЄС також визначають ШІ пріоритетом національної безпеки і оборони. Наприклад, 2022 році Міністерство Збройних Сил Франції схвалило останню фазу платформи обробки великих даних Artemis, розробленої для забезпечення автономних операцій у розвідувальній, командній та цифровій сферах. Франція планує побудувати найпотужніший у Європі секретний суперкомп'ютер, щоб взяти на себе лідерство у сфері ШІ для оборонних цілей. У травні 2024 року Франція заснувала Міністерське агентство ШІ в обороні з бюджетом 300 мільйонів євро. Французький оборонний стартап Mistral нещодавно об'єднався з німецьким оборонним стартапом Helsing для розробки передових військових систем ШІ [16].

Варто також відзначити, що у ЄС виникають занепокоєння щодо критичних аспектів регулювання ШІ, наприклад стосовно систем розпізнавання емоцій, біометричної категоризації та практики соціального скорингу. Біометрична ідентифікація в режимі реального часу стала спірною сферою, зокрема щодо цілей правоохоронних органів. Науковий і практичний дискурс відбувається навколо необхідності суворих обмежень та нагляду для запобігання масовому спостереженню.

Окремі негативні приклади використання систем ШІ в ЄС свідчать про посилення спостереження та втручання без конкретних доказів злочинної діяльності. Такі випадки були зафіксовані у системах ШІ "Top 600" і ProKid у Нідерландах, RisCanvi в Каталонії, які розроблені для прогнозування злочинної поведінки або оцінки ризику рецидивізму. Багато систем працюють з мінімальним людським наглядом, що ускладнює розуміння того, як приймаються рішення. Ці системи часто призводять до поліцейських рейдів або посиленого спостереження, що ґрунтуються виключно на алгоритмічних прогнозах, а не на перевірених доказах правопорушень [30].

Країни-члени ЄС, наприклад Німеччина, активно розвивають використання ШІ в системі правосуддя. Цифровізація системи правосуддя у Німеччині з використанням ШІ автоматизує повторювані завдання, спрощуючи етапи обробки та полегшуючи доступ до правосуддя для всіх. Коаліційна угода міністрів юстиції уряду Німеччини разом з урядами земель передбачає створення комісії з реформ для модернізації чинного кримінально-процесуального законодавства. Федеральний уряд інвестуватиме значні ресурси для спільного із землями Німеччини просування проектів цифровізації, що покращить доступ до правосуддя та зробить роботу в судах та прокуратурі більш ефективною. Німецька судова система вже використовує деякі програми на основі ШІ в різних сферах. Використання систем ШІ в судовій системі наразі просувається в рамках кількох проектів, деякі з яких також фінансуються за рахунок федеральних коштів у межах Ініціативи цифровізації судової влади [31].

У свою чергу Швеція лише розвиває комплексну стратегію щодо ШІ, яка має бути завершена до 2026 року. Відносно невеликий внутрішній ринок Швеції обмежує масштаби, в яких шведські компанії можуть розробляти та тестувати рішення ШІ. Уряд Швеції влітку 2024 року доручив шведському органу із захисту даних [32] разом зі шведським Агентством цифрового управління [33] розробити вказівки щодо сприяння ефективному та належному використанню генеративного ШІ у державному управлінні.

Висновки. Підсумовуючи викладене, зазначимо, що відсутність правового регулювання щодо ШІ і неналежне правозастосування, коли таке регулювання впроваджено, може спричинити негативний вплив на права людини та суспільство в цілому. Оскільки системи ШІ все більше інтегруються у повсякденне життя та економіку, потенційні наслідки недотримання правових вимог виходитимуть за межі сфери ШІ.

У статті доведено, що на сьогодні відсутні міжнародно-правові імперативні нормативи у сфері ШІ, а система правового регулювання ШІ у США послабилася після скасування Указу №14110 про безпечну, захищену та надійну розробку та використання ШІ. Фактично неконтрольоване і необмежене використання ШІ як у новітніх продуктах великих ІТ компаній, так і у державних структурах США може спровокувати загрозу порушення прав людини і навіть національних інтересів інших держав.

Основний конкурент США у сфері ШІ – Китай призупинив розробку проекту Закону “Про штучний інтелект”. Як наслідок, проблеми конфіденційності та безпеки даних ШІ DeepSeek, розробленої у Китаї, спричинили заборону цього продукту в кількох країнах і державних установах через загрози національній безпеці, зокрема через потенційний доступ китайського уряду до даних, що збирає DeepSeek.

Здійснений аналіз законодавства Китаю дає підстави для висновку, що у цій державі існує значний державний контроль за сферою генеративних послуг ШІ, зокрема послуг “глибоких фейків” (“deep fake”) з вимогами для провайдерів обов’язкового інформування Міністерства громадської безпеки Китаю.

Зроблено висновок, що законодавство ЄС щодо ШІ містить механізми захисту прав людини від імовірного негативного впливу внаслідок розробки і використання систем ШІ. Саме Закон ЄС про ШІ та інфраструктура нагляду, що наразі формується, є гарантією дотримання прав людини у цій чутливій сфері.

Перспективами подальших наукових пошуків визначаємо питання розкриття принципів правового регулювання відносин щодо ШІ у окремих зарубіжних країнах.

Список використаних джерел

[1] І. С. Пирога і Ю. Ф. Волкова, «Право на використання технологій штучного інтелекту: нові виклики та загрози для людини», *Науковий вісник Ужгородського національного університету. Серія: Право*, вип. 1, вип. 84, с. 138–143, Вер 2024, doi: 10.24144/2307-3322.2024.84.1.20.

[2] N. O. Popova, «International legal regulation of artificial intelligence: current status and prospects», *Juridical scientific and electronic journal*, вип. 4, с. 443–447, 2024, doi: 10.32782/2524-0374/2024-4/105.

[3] І. Макух-Федоркова і Д. Мікіцел, «Правові засади розвитку штучного інтелекту: європейський та американський досвід», *Медіафорум : аналітика, прогнози, інформаційний менеджмент*, вип. 15, с. 304–319, Груд 2024, doi: 10.31861/mediaforum.2024.15.304-319.

[4] О. С. Котуха і Д. І. Попов, «Штучний інтелект та права людини: проблеми цифровізації права на сучасному етапі розвитку електронної держави», *Вісник ЛТЕУ. Юридичні науки*, вип. 15, с. 19–27, Лип 2024, doi: 10.32782/2616-7611-2024-15-03.

[5] B. Judge, M. Nitzberg, і S. Russell, «When code isn’t law: rethinking regulation for artificial intelligence», *Policy Soc*, вип. 44, вип. 1, с. 85–97, Квіт 2025, doi: 10.1093/polsoc/puae020.

[6] «The issues of legal regulation of artificial intelligence», в *ResearchGate*. Дата звернення: 27, Серпень 2025. [Online]. Доступний у: https://www.researchgate.net/publication/381916791_The_issues_of_legal_regulation_of_artificial_intelligence

[7] G. Finocchiaro, «The regulation of artificial intelligence», *AI & Soc*, вип. 39, вип. 4, с. 1961–1968, Сер 2024, doi: 10.1007/s00146-023-01650-z.

[8] A. Marushchak, S. Petrov, і A. Khoperiya, «Countering AI-powered disinformation through national regulation: learning from the case of Ukraine», *Front. Artif. Intell.*, вип. 7, Січ 2025, doi: 10.3389/frai.2024.1474034.

[9] «Homepage | Global Digital Compact». Дата звернення: 27, Серпень 2025. [Online]. Доступний у: https://www.un.org/global-digital-compact/en

[10] «OHCHR | Call for input of the Special Rapporteur on the independence of judges and lawyers for her next thematic report on artificial Intelligence and judicial systems», OHCHR. Дата звернення: 27, Серпень 2025. [Online]. Доступний у: https://www.ohchr.org/en/calls-for-input/2025/call-input-special-rapporteur-independence-judges-and-lawyers-her-next

[11] «Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence», Federal Register. Дата звернення: 27, Серпень 2025. [Online]. Доступний у: https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

[12] E. Tabassi, «Artificial Intelligence Risk Management Framework (AI RMF 1.0)», National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST AI 100-1, Січ 2023. doi: 10.6028/NIST.AI.100-1.

[13] «America’s AI Action Plan». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[14] «CDAO Re-alignment to USD(R&E) Accelerates AI Transformation at DoD», Chief Digital and Artificial Intelligence Office. Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.ai.mil/Latest/News-Press/PR-View/Article/4281147/cdao-re-alignment-to-usdre-accelerates-ai-transformation-at-dod/

[15] «AI Cyber Challenge marks pivotal inflection point for cyber defense | DARPA». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.darpa.mil/news/2025/aixcc-results

[16] «Defence and artificial intelligence». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)769580.

[17] «Full Translation: China’s ‘New Generation Artificial Intelligence Development Plan’ (2017)», DigiChina. Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[18] «DeepSeek AI | Leading AI Language Models & Solutions». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://deepseek.ai/

[19] S. Han, «The Frontier Illusion: Rethinking DeepSeek’s AI Threat», Internet Governance Project. Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.internetgovernance.org/2025/02/21/the-frontier-illusion-rethinking-deepseeks-ai-threat/

[20] «AI Watch: Global regulatory tracker - China | White & Case LLP». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china

[21] «Cybersecurity technology — Generative artificial intelligence data annotation securitys pecification». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://content.mlex.com/Attachments/2025-05-23_CZT297CHX8R49J68/SAMR_NSA_GenAI_data_annotation_security_specification.pdf

[22] «Cybersecurity technology — Security specification for generative artificial intelligence pre-training and fine-tuning data». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://content.mlex.com/Attachments/2025-05-23_CZT297CHX8R49J68/SAMR_NSA_Security_Specification_GenAI_pre-training_fine-tuning_Data.pdf

[23] «Cybersecurity technology — Basic security requirements for generative artificial intelligence service». Дата звернення: 30, Серпень 2025. [Online]. Доступний у:

https://content.mlex.com/Attachments/2025-05-23_CZT297CHX8R49J68/SAMR_NSA_Basic_Security_Requirements_GenAI_service.pdf

[24] «The AI Act Explorer | EU Artificial Intelligence Act». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://artificialintelligenceact.eu/ai-act-explorer/

[25] «AI continent - European Commission». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://commission.europa.eu/topics/eu-competitiveness/ai-continent_en

[26] «The General-Purpose AI Code of Practice | Shaping Europe's digital future». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

[27] «Explanatory Notice and Template for the Public Summary of Training Content for general-purpose AI models | Shaping Europe's digital future». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models

[28] «European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

[29] «PESCO | Member States Driven». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.pesco.europa.eu/

[30] «EUSurvey - Survey X». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://cdt.org/wp-content/uploads/2025/08/CDT-Europe-response-to-the-high-risk-AI-systems-consultation.pdf

[31] «HdR - Pressemitteilungen - Sechster Bund-Länder-Digitalgipfel der Justizministerinnen und Justizminister: Gemeinsame Erklärung zum Einsatz von Künstlicher Intelligenz in der Justiz». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://hdr4.bmj.de/SharedDocs/Pressemitteilungen/DE/2025/0605_Digitalgipfel.html

[32] «Swedish Authority for Privacy Protection | IMY». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.imy.se/en/

[33] «Agency for Digital Government». Дата звернення: 30, Серпень 2025. [Online]. Доступний у: https://www.digg.se/en

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