ISSN 2524-0374

УДК 004.056:342.7
DOI https://doi.org/10.32782/2524-0374/2025-11/33

ЛЮДСЬКИЙ ЕЛЕМЕНТ У СИСТЕМАХ ШІ, ЩО ОБРОБЛЯЮТЬ ПЕРСОНАЛЬНІ ДАНІ: ЄВРОПЕЙСЬКИЙ СТАНДАРТ І УКРАЇНСЬКИЙ ДЕФІЦИТ РЕГУЛЮВАННЯ

THE HUMAN ELEMENT IN AI SYSTEMS PROCESSING PERSONAL DATA: EUROPEAN STANDARD AND UKRAINIAN REGULATORY DEFICIT

Машталяр О.М., аспірант кафедри інформаційних технологій
Навчально-науковий інститут права та психології Національної академії внутрішніх справ
orcid.org/0009-0009-6979-333X

Хахановський В.Г., д.ю.н., професор,
професор кафедри інформаційних технологій
Навчально-науковий інститут права та психології Національної академії внутрішніх справ
orcid.org/0000-0001-5676-5641

Мета дослідження полягає у визначенні ролі «людського елементу» в системах штучного інтелекту, що обробляють персональні дані, на основі аналізу європейських стандартів (GDPR, Акту ЄС про ШІ) та оцінки нормативного вакууму в Україні. У дослідженні застосовано методи порівняльно-правового аналізу, системного аналізу нормативних актів ЄС і національного законодавства, а також кейс-стаді (аналіз судового рішення CJEU у справі SCHUFA). У роботі вперше комплексно проаналізовано концепцію людиноцентричного регулювання ШІ в ЄС у контексті персональних даних та виявлено прогалини українського законодавства у цій сфері; запропоновано конкретні шляхи його вдосконалення з урахуванням європейського досвіду. Установлено, що Європейський Союз сформував цілісний підхід до залучення людини на всіх етапах функціонування високоризикових ШІ-систем: GDPR гарантує фізичним особам право на перегляд автоматизованих рішень людиною, а Акт про ШІ запроваджує обов'язковий людський нагляд за системами з високим рівнем ризику. Проаналізовано прецедентну практику (справа CJEU SCHUFA), яка підтвердила ключову роль людського контролю в автоматизованому кредитному скорингу. Виявлено, що в Україні спеціальне правове регулювання використання ШІ відсутнє: діють лише загальні норми Закону України «Про захист персональних даних» (2010), які декларують право на захист від суто автоматизованих рішень, але не містять механізмів реалізації цього права. Водночас окреслено позитивні зрушення: розроблено нову редакцію закону про персональні дані (наближену до GDPR) та концептуальні документи щодо регулювання ШІ. Людиноцентричний підхід до регулювання ШІ є критично важливим для захисту прав людини в цифрову епоху. Україні доцільно імплементувати європейські стандарти залучення людини – закріпити на законодавчому рівні право на втручання людини в автоматизовані процеси, вимоги до прозорості та підзвітності алгоритмів, а також створити інституційні механізми нагляду за ШІ. Це сприятиме підвищенню довіри до систем ШІ та забезпечить баланс між технологічними інноваціями й правами людини.

Ключові слова: персональні дані, автоматизоване рішення, штучний інтелект, GDPR, Акт про ШІ, людський нагляд, право на втручання, регулювання, Європейський Союз, Україна.

The purpose of this study is to determine the role of the "human element" in artificial intelligence (AI) systems that process personal data by analyzing European standards (the GDPR and EU AI Act) and assessing the regulatory gaps in Ukraine. The research methodology includes comparative legal analysis, a systematic review of EU and Ukrainian legal acts, and a case study of relevant jurisprudence (the CJEU SCHUFA decision). The study offers a first comprehensive analysis of the human-centric approach to AI regulation in the EU within the context of personal data, and identifies gaps in Ukrainian legislation in this domain; based on this analysis, concrete directions for improving Ukraine's legal framework are proposed in light of European experience. The analysis demonstrates that the European Union has developed a holistic approach to ensuring human involvement at all stages of high-risk AI systems. The GDPR guarantees individuals the right to human review of automated decisions, while the AI Act introduces mandatory human oversight for high-risk AI applications. European case law (notably the CJEU's SCHUFA ruling) confirms the pivotal role of human control in automated credit scoring and similar processes. It is found that Ukraine currently lacks dedicated legal regulation for the use of AI: only the general provisions of the 2010 Law "On Personal Data Protection" apply, which declare a right to protection from purely automated decisions but provide no mechanisms for its implementation. At the same time, some positive steps are noted: a new draft personal data law (harmonized with the GDPR) has been developed, and strategic documents on AI regulation have been introduced. A human-centric approach to AI governance is critically important for safeguarding human rights in the digital age. It is recommended that Ukraine implement European standards of human involvement—enshrining the right to human intervention in automated processes, requirements for algorithmic transparency and accountability, and establishing institutional mechanisms for AI oversight. Such measures will increase public trust in AI systems and ensure a balance between technological innovation and individual rights.

Key words: personal data, automated decision-making, artificial intelligence, GDPR, AI Act, human oversight, right to intervention, regulation, European Union, Ukraine.

Вступ. Стрімкий розвиток технологій штучного інтелекту суттєво впливає на сфери обробки персональних даних. Алгоритми здатні автоматизувати ухвалення рішень – від кредитного скорингу до відбору кандидатів на роботу – що підвищує ефективність процесів, але водночас породжує нові правові та етичні виклики. Одним із ключових питань є збереження «людського елементу», тобто участі людини в системах ШІ, які обробляють персональні дані. Надмірна автоматизація без належного людського контролю може призвести до порушень прав осіб – від дискримінації через алгоритмічну упередженість до неможливості оскаржити помилкове рішення машини. Європейський Союз реагує на ці виклики шляхом запровадження людиноцентричних підходів до регулювання ШІ. Зокрема, у етичних настановах з питань довірчого ШІ (2019) незалежна Група високого рівня ЄС з питань ШІ визначила принцип «людської автономії та нагляду» першим серед семи ключових вимог до довірчого ШІ [1, с. 14]. Відповідно, у правовому полі ЄС пріоритет надається забезпеченню того, щоб остаточний контроль за важливими рішеннями, що ухвалюються ШІ-системами, залишався за людиною.

У цій статті проаналізовано європейські нормативні стандарти стосовно ролі людини при автоматизованій

© Машталяр О.М., Хахановський В.Г., 2025
Стаття поширюється на умовах ліцензії CC BY 4.0

обробці персональних даних – передусім вимоги GDPR та Акту про ШІ – а також судову практику, що їх конкретизує. Окрему увагу приділено стану українського законодавства: виявлено наявність прогалин (дефіциту спеціального регулювання) та запропоновано напрямки його вдосконалення з урахуванням європейського досвіду.

Європейський стандарт залучення людини в AI-системах з персональними даними GDPR: право на людське втручання при автоматизованих рішеннях. Базовим європейським актом у сфері захисту персональних даних є Регламент (ЄС) 2016/679 (GDPR) [2, с. 14]. Стаття 22 GDPR закріплює загальне правило, за яким суб'єкт даних має право не підлягати рішенню, що базується виключно на автоматизованій обробці, якщо таке рішення породжує для нього правові наслідки або істотно на нього впливає [3, с. 15]. Іншими словами, важливі рішення не можуть бути повністю віддані на відкуп алгоритму без можливості людини переглянути або скоригувати їх. GDPR передбачає лише вузькі винятки з цього принципу. Зокрема, автоматизоване рішення без участі людини є допустимим, якщо воно:

– необхідне для укладення або виконання договору між суб'єктом даних і контролером;

– дозволене законом ЄС або держави-члена, який також передбачає відповідні гарантії захисту прав суб'єкта;

– здійснюється на підставі явної згоди суб'єкта даних [3, с. 15].

Навіть у випадках, коли автоматизоване ухвалення рішення законно на підставі зазначених винятків, GDPR вимагає впровадження додаткових захисних заходів. Зокрема, контролер зобов'язаний забезпечити як мінімум право суб'єкта даних на втручання людини в процес ухвалення рішення, право висловити свою точку зору та право оскаржити це рішення [3, с. 15]. Таким чином, європейський стандарт виходить з концепції **«human in the loop»**, за якою остаточне рішення не має ухвалюватися виключно машиною без можливості його додаткового осмисленого перегляду людиною. Від людини вимагається не формальне схвалення результату алгоритму, а саме осмислене втручання – аналіз і за необхідності коригування автоматичного рішення уповноваженою особою, компетентною змінити цей результат. Як підкреслила Робоча група зі статті 29 (у своїх Керівних принципах щодо автоматизованого ухвалення рішень, 2018 р.), втручання повинно бути «meaningful», тобто здійснюватися реально, а не декларативно [4, с. 15].

Закріплення права на людське втручання в GDPR пов'язане з усвідомленням потенційних ризиків автоматизованого профілювання та прийняття рішень, заснованих виключно на алгоритмах. Європейські регулятори наполягають, що навіть за наявності згоди особи або іншої законної підстави, особа не повинна залишатися сам на сам із «чорним ящиком» алгоритму. Вона має право отримати пояснення логіки рішення і вимагати перегляду його людиною. Практичне значення цієї норми підтверджується судовою практикою. Так, у справі **C-634/21 SCHUFA Holding AG** (2023) Суд ЄС роз'яснив застосування статті 22 GDPR до кредитного скорингу. **SCHUFA** – найбільше кредитне бюро Німеччини – автоматично обчислює бали платоспроможності осіб. У випадку позивачки, якій банк відмовив у кредиті на підставі низького скорингового балу, постало питання: чи вважається формування такого балу автоматизованим рішенням, забороненим GDPR? SCHUFA стверджувала, що вона лише здійснює «підготовчі дії», а остаточне рішення (відмова у кредиті) ухвалює банк-активіст. Однак Суд ЄС відхилив таку аргументацію, постановивши, що обчислення кредитного рейтингу, на який кредитори покладаються вирішальною мірою, само по собі є автоматизованим індивідуальним рішенням у розумінні статті 22(1) GDPR [5, с. 15]. Отже, діяльність бюро кредитних історій підпадає під обмеження статті 22, а відповідні обробки даних заборонені, якщо не наявний виняток. Суд наголосив, що національне законодавство (як-от німецький Федеральний закон про захист даних) може передбачати виняток із заборони solo-автоматизованих рішень лише за умов суворої відповідності вимогам GDPR [5, с. 15]. У будь-якому разі, навіть за наявності правової підстави, суб'єкту даних мають бути гарантовані права, передбачені ст.22(3) GDPR, зокрема право вимагати перегляду рішення людиною. Таким чином, SCHUFA-прецедент фактично підтвердив центральність «людського елементу»: якщо рішення значною мірою ґрунтується на автоматичному скорингу, людина повинна мати можливість втрутитись, висловитись і добитися зміни рішення. Це рішення вже охарактеризоване як таке, що матиме вплив на всі сервіси автоматизованого ухвалення рішень, які пропонують прогнозні інструменти ШІ [6, с. 15]. Хоча деякі коментатори вважають такі оцінки перебільшенням, сам факт втручання найвищого судового органу ЄС підкреслює важливість дотримання принципу *human-in-the-loop* у практиці використання ШІ.

Акт ЄС про ШІ: вимоги людського нагляду за високоризиковими системами. Наступним кроком після GDPR стало формування спеціального режиму регулювання штучного інтелекту в ЄС. У червні 2024 р. завершено ухвалення Регламенту (ЄС) 2024/1689 «Акт про штучний інтелект» (AI Act) – першого комплексного закону про ШІ [7, с. 15]. Акт про ШІ запроваджує ризик-орієнтований підхід: системи ШІ поділяються на неприйнятні, високого ризику, обмеженого ризику та мінімального ризику. Найбільш значущі вимоги встановлено для високоризикових ШІ-систем, до яких, зокрема, віднесено системи, що використовуються для оцінки кредитоспроможності, в управлінні персоналом, у сфері правосуддя, біометричної ідентифікації, в критичній інфраструктурі тощо. Однією з ключових вимог для таких систем є людський нагляд (oversight) за їх функціонуванням. Згідно з статтею 14 Акта, високоризикова ШІ-система повинна бути спроектована таким чином, щоб протягом усього періоду використання забезпечувати ефективний нагляд з боку людини [8, с. 15]. Мета людського нагляду – попередити або мінімізувати ризики для життя, безпеки чи фундаментальних прав, що можуть виникнути при застосуванні ШІ [8, с. 15].

Акт про ШІ встановлює конкретні вимоги до реалізації людського нагляду. Заходи з нагляду мають відповідати рівню ризику, контексту використання і автономності системи [8, с. 15]. Вони можуть бути як технічно вбудованими в систему виробником, так і реалізованими на рівні користувача (деплойера) через організаційні процедури [8, с. 15]. ШІ-система повинна надаватися таким чином, щоб відповідальні особи (оператори), на яких покладено нагляд, були здатні:

– розуміти релевантні можливості та обмеження системи;

– моніторити її роботу і виявляти аномалії, збої чи непередбачувані результати;

– усвідомлювати ризик автоматичної надмірної довіри до рекомендацій ШІ (так званий *automation bias*);

– правильно інтерпретувати результати, що надає система (з урахуванням доступних інструментів пояснення);

– прийняти рішення не використовувати систему у конкретному випадку або ігнорувати/відхилити отриманий від неї результат;

– втрутитися в роботу системи чи зупинити її (наприклад, через «червону кнопку» аварійної зупинки) [8, с. 15].

Таким чином, європейський закон про ШІ робить акцент на постійній участі людини у експлуатації алгоритмів, що можуть впливати на права людей. Додатково для окремих категорій систем встановлено спеціальні

вимоги. Наприклад, для систем біометричної ідентифікації в режимі реального часу (в громадських місцях) Акт про ШІ вимагає, щоб кожне рішення на основі автоматичної ідентифікації особи перевірялося і підтверджувалося щонайменше двома уповноваженими людьми перед вчиненням дії [8, с. 15]. Хоча ця вимога має винятки (зокрема, для правоохоронних органів у визначених випадках), її наявність підкреслює принцип: у сферах підвищеної чутливості машинний висновок не може бути єдиною підставою дії без подвійної перевірки людиною.

Варто зауважити, що концепції «human oversight» (людський нагляд), запроваджені AI Act, і «human intervention» (людське втручання), закріплені в GDPR, мають різне техніко-юридичне значення [4, с. 15]. GDPR гарантує суб'єкту даних право на людський перегляд уже ухваленого рішення (тобто *ex post* втручання), тоді як Акт про ШІ вимагає організації проактивного нагляду за роботою системи ШІ з боку операторів (*ex ante* та *in real time*). Обидва підходи доповнюють один одного і разом формують європейський стандарт: «жодна система ШІ, що суттєво впливає на права людей, не повинна діяти без відповідного людського контролю».

Європейська практика: приклад справи SCHUFA і наслідки для регулювання. Як уже розглянуто вище, рішення CJEU у справі SCHUFA висвітлило важливість дотримання вимог статті 22 GDPR на практиці кредитного скорингу. Цей прецедент став сигналом для всіх постачальників алгоритмічних систем ухвалення рішень: відповідальність за дотримання обмежень автоматизованого профілювання несе не тільки кінцевий користувач (наприклад, банк), але й розробник/постачальник скорингової моделі [6, с. 15]. Після рішення SCHUFA регулятори ЄС наголосили, що подібні моделі штучного інтелекту мусять бути переглянуті на відповідність GDPR, адже суб'єкти даних повинні мати механізми захисту – право знати логіку, оскаржувати оцінку і вимагати участі людини при вирішенні їх долі.

Іншим аспектом є *транспарентність* роботи алгоритмів. У випадку SCHUFA, позивачка вимагала від кредитного бюро розкрити методику розрахунку скорингового балу, але компанія відмовилася, пославшись на комерційну таємницю [6, с. 15]. Суд ЄС у цьому провадженні зосередився на питанні автоматизованого ухвалення рішення, а не прозорості, але загальноєвропейська дискусія продовжується: як збалансувати право на пояснення рішення ШІ з правами інтелектуальної власності на алгоритми. Певні орієнтири надає все той же Акт про ШІ, який містить вимоги до задокументованості і пояснюваності високоризикових систем (статті 13 та 15 AI Act). Так, розробники повинні надавати користувачам інструкції щодо інтерпретації виходів системи, характеру використаних даних, рівня точності тощо. Це доповнює вимоги GDPR і дає людині більше інструментів для здійснення ефективного контролю.

Підсумовуючи, європейський стандарт можна охарактеризувати як такий, що поєднує право індивіда на втручання людини (як гарантію проти суто автоматизованих рішень) та обов'язок постачальників і користувачів забезпечити постійний нагляд людини за функціонуванням алгоритмів. Такий підхід впроваджується як нормативно (через GDPR, майбутній AI Act та інші акти), так і через м'яке право – етичні настанови, кодекси поведінки, роз'яснення наглядових органів. Важливо, що Європа формує глобальний порядок денний у цій сфері: концепція «AI, що підзвітний людині» стає частиною міжнародних стандартів і обговорень.

Український контекст: дефіцит регулювання і перспективи розвитку. На відміну від ЄС, в Україні спеціальне правове регулювання використання систем ШІ тільки починає формуватися. Наразі відсутній окремий нормативний акт, який би врегульовував відносини, пов'язані зі штучним інтелектом. Правове поле обмежується загальними нормами, передусім Законом України «Про захист персональних даних» 2010 р. Цей закон містить лише кілька положень, дотичних до нашої тематики. Зокрема, стаття 8 (права суб'єкта даних) гарантує особі право «на захист від автоматизованого рішення, що має для неї правові наслідки» [9, с. 15]. Таким чином, закріплено принцип, подібний до положень статті 22 GDPR: людина має бути захищена від повністю автоматизованих рішень. Однак ані механізм реалізації цього права, ані критерії допустимості таких рішень українським законом не розкриті. Фактично, норма носить декларативний характер – на практиці відсутні підзаконні акти чи роз'яснення, які б регулювали процедуру перегляду автоматизованих рішень або встановлювали винятки. До того ж, дієвого контролю за дотриманням цієї норми немає: спеціального органу із захисту персональних даних в Україні поки що не створено (функції наглядового органу виконує Уповноважений Верховної Ради з прав людини, але без достатніх ресурсів і повноважень як у європейських DPA).

Українські науковці та фахівці звертають увагу на небезпеки, пов'язані з неврегульованим впровадженням ШІ. Зазначається, що вже зараз алгоритми використовуються у чутливих сферах (наприклад, системи відеоспостереження з розпізнаванням обличчя, автоматизовані системи оцінки платоспроможності позичальників тощо), і брак чітких правових норм та етичних рамок створює ризики порушення прав громадян[10, с. 16]. Під час фахових обговорень наголошується на необхідності забезпечити людський контроль та можливість перегляду рішень, що ухвалюються автоматизованими системами. Так, суддя Верховного Суду Я. Берназюк, аналізуючи перспективи застосування ШІ в судочинстві, підкреслив, що *«відсутність перегляду рішень ШІ»* є неприйнятною, і важливо гарантувати участь людини в процесі ухвалення судових рішень, якщо застосовуються алгоритми [11, с. 16]. Ця думка відображає загальне усвідомлення: ШІ має допомагати, але не заміняти людину там, де йдеться про реалізацію прав і свобод.

На шляху до євроінтеграції Україна поступово імплементує європейські стандарти і в цій сфері. У 2023–2024 рр. зроблено важливі кроки до адаптації законодавства про захист персональних даних. Зокрема, у листопаді 2024 р. парламент прийняв у першому читанні нову редакцію Закону «Про захист персональних даних» (законопроект № 8153), покликану гармонізувати національні норми з GDPR та Конвенцією 108+ [12, с. 16]. Цей проект закону прямо забороняє автоматизоване рішення, що створює значні правові наслідки для особи, без належних гарантій. Він детальніше регулює питання профілювання та автоматизованих рішень: надає суб'єкту даних право бути проінформованим про факт і логіку автоматизованої обробки, вводить визначення «профілювання» за зразком GDPR, передбачає проведення оцінки впливу на захист даних (DPIA) у разі масштабного автоматизованого оброблення з високим ризиком[13, с. 16]. Інакше кажучи, українське законодавство наближається до вимог статті 22 GDPR – з усіма її винятками та гарантіями. Проте станом на кінець 2025 р. цей проєкт ще не набув чинності, отже реальні механізми забезпечення права на людський перегляд автоматизованих рішень залишаються неуведені.

Окрім оновлення закону про персональні дані, Україна розробляє підходи до регулювання ШІ в цілому. Урядові документи стратегічного характеру – **Концепція розвитку штучного інтелекту** (схвалена наприкінці 2020 р.) та **Дорожня карта з регулювання ШІ** (оприлюднена Міністерством цифрової трансформації у жовтні 2023 р.) – фіксують наміри держави створити умови для етичного і правового впровадження ШІ. Зокрема, у Дорожній карті передбачено поетапний підхід: спершу напрацювання практики використання ШІ у різних сферах, а згодом –

розробка спеціального законодавчого акту, що поступово імплементує положення Європейського Акта про ШІ в національне право. Таким чином, уже офіційно задекларовано курс на врахування європейських нормативних новацій, включно з вимогами щодо людського нагляду за ШІ. Показово, що у світовому рейтингу готовності урядів до ШІ (Government AI Readiness Index 2023) Україна посіла 60-те місце зі 172, випередивши навіть деякі країни Західної Європи [9, с. 15]. Експерти відзначили наявність у нашій країні стратегічного бачення та елементів етичної і регуляторної бази, хоча й наголосили, що повноцінна реалізація потребує часу.

Отже, **дефіцит українського регулювання** в сфері людського фактору при використанні ШІ наразі є очевидним. В національному законодавстві бракує як детальних процедурних механізмів (хто і як повинен здійснювати людський перегляд автоматичних рішень), так і інституційного забезпечення (спеціального органу контролю). Тим не менш, узятий курс на євроінтеграцію обумовлює поступове усунення цих прогалин. Вже невдовзі очікується прийняття нової редакції закону про персональні дані, що зблизить правила гри з європейськими. Наступним кроком має стати розробка законодавства про штучний інтелект – можливо, окремого закону чи включення норм до існуючих актів – де будуть враховані підходи ЄС щодо класифікації ризиків, обов'язків розробників і користувачів ШІ, вимоги до сертифікації тощо. При цьому критично важливо передбачити на національному рівні ті гарантії «людяності» ШІ, що стали нарізним каменем у Європі: незалежно від технічної складності системи, людина повинна зберігати контроль над її результатами, а особа – мати право на справедливе рішення з урахуванням людського судження.

Європейський досвід чітко демонструє: **присутність людини в контурі ухвалення рішень ШІ є необхідною умовою захисту прав людини в цифрову епоху**. GDPR встановив базовий принцип, що важливі рішення не можуть прийматися суто алгоритмами без можливості людського втручання, а розроблюваний Акт про ШІ поглибив цей підхід, зобов'язавши провайдерів та користувачів високоризикових систем забезпечувати ефективний людський нагляд. Судова практика ЄС (справа SCHUFA та ін.) підтвердила готовність регуляторів притягувати до відповідальності суб'єктів, які покладаються на «сліпі» автоматизовані рішення без належних запобіжників для індивідів.

В Україні натомість спеціальне регулювання поки відстає від технологічних реалій: норми закону про персональні дані про «захист від автоматизованих рішень» лишаються швидше декларацією, не підкріпленою механізмами реалізації. Це становить ризики, адже системи ШІ вже впроваджуються у різних галузях – від фінансів до безпеки – і відсутність чітких правил гри може призвести до зловживань та порушення прав громадян. Український дефіцит регулювання в цій сфері слід якнайшвидше заповнити, використовуючи найкращі європейські практики. Першочергово необхідно ухвалити новий закон про захист даних, який відобразить норми GDPR, включно з правом на людське втручання та вимогами до прозорості алгоритмів. Паралельно варто розробити дорожню карту імплементації основних положень Акта про ШІ – з урахуванням національних особливостей – аби підготувати ґрунт для повноцінного правового регулювання ШІ. Важливим є створення незалежного регуляторного органу (аналога європейських data protection authorities), який би опікувався як захистом персональних даних, так і наглядом за етичною розробкою і застосуванням ШІ.

Підсумовуючи, **людський елемент має стати невід'ємною складовою української екосистеми ШІ**. Це відповідає як суспільним очікуванням (забезпечення справедливості та контролю над технологіями), так і міжнародним зобов'язанням України в рамках євроінтеграції. Запозичення європейського стандарту – де права людини є центральними, а технології слугують, а не панують – дозволить Україні розвивати штучний інтелект без загрози для прав і свобод, зберігаючи довіру громадян до новітніх систем. У перспективі це сприятиме і інноваційному розвитку, адже довірчий, підзвітний людині ШІ є запорукою сталого впровадження технологій у всі сфери життя.

ЛІТЕРАТУРА

1. Ethics guidelines for trustworthy AI. High-Level Expert Group on Artificial Intelligence. Brussels: European Commission, 2019. URL: https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf (дата звернення: 31.10.2025).
2. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС. Дата оновлення: 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 31.10.2025).
3. Art. 22 GDPR – Automated individual decision-making, including profiling. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/art-22-gdpr/ (дата звернення: 31.10.2025).
4. Human intervention and human oversight in the GDPR and AI. Trilateral Research. 31 травня 2022. URL: https://trilateralresearch.com/emerging-technology/human-intervetion-in-gdpr-and-ai (дата звернення: 30.10.2025).
5. The General Data Protection Regulation (GDPR) opposes two data processing practices by credit information agencies. Court of Justice of the European Union. 07 грудня 2023. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-12/cp230186en.pdf (дата звернення: 29.10.2025).
6. Boardman R. Key takeaways from the CJEU's recent automated decision-making rulings. IAPP. 19 грудня 2023. URL: https://iapp.org/news/a/key-takeaways-from-the-cjeus-recent-automated-decision-making-rulings (дата звернення: 29.10.2025).
7. Regulation (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/eli/reg/2024/1689/oj/eng (дата звернення: 31.10.2025).
8. Article 14: Human oversight. EU Artificial Intelligence Act. URL: https://artificialintelligenceact.eu/article/14/ (дата звернення: 28.10.2025).
9. Січкар А. Євроінтеграція: регулювання штучного інтелекту в Україні та ЄС. ЮРЛІГА. 11 червня 2024. URL: https://jurliga.ligazakon.net/analitycs/228365_vrontegratsya-regulyuvannya-shtuchnogo-ntelektu-v-ukran-ta-s (дата звернення: 30.10.2025).
10. Несенко А. Погано дивитися лише на ЄС. «Біла книга» регулювання штучного інтелекту від Мінцифри розчарувала бізнес. Чому: Forbes зібрав п'ять претензій до документу. Forbes Україна. 05 липня 2024. URL: https://forbes.ua/innovations/pogano-divitisya-lishe-na-es-bila-kniga-regulyuvannya-shtuchnogo-intelektu-vid-mintsifri-rozcharuvala-biznes-chomu-forbes-zibrav-pyat-pretenziy-do-dokumentu-05072024-22227 (дата звернення: 27.10.2025).
11. Берназюк Я. Штучний інтелект та право на приватність: баланс між інноваціями та захистом персональних даних: презентація PowerPoint. Верховний Суд. Київ. 20 лютого 2025. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/119_AI_personal_data_protection_bernaziuk.pdf (дата звернення: 29.10.2025).
12. Baker McKenzie. Key Data & Cybersecurity Laws: Ukraine. Global Data and Cyber Handbook. 23 грудня 2024. URL: https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/ukraine/topics/key-data-and-cybersecurity-laws (дата звернення: 26.10.2025).
13. Data Protection Laws and Regulations Report 2025: Ukraine. ICLG Data Protection. 21 липня 2025. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/ukraine (дата звернення: 31.10.2025).

Дата першого надходження рукопису до видання: 21.11.2025
Дата прийнятого до друку рукопису після рецензування: 11.12.2025
Дата публікації: 30.12.2025