АКАДЕМІЧНІ ВІЗІЇ
Випуск 55/2026

Секція Право	
УДК 340:004.8:342.7(477)	
Дата першого надходження статті до видання	2026-04-21
Дата прийняття статті до друку після рецензування	2026-05-30
Дата публікації/оприлюднення	2026-05-30

ОЦІНКА ВПЛИВУ ВИСОКОРИЗИКОВИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ ЯК ІНСТРУМЕНТ ПРАВОВОЇ ПОЛІТИКИ УКРАЇНИ

Владислав Олексійович ВАРИНСЬКИЙ
Доцент кафедри філософії та україністики Національного університету «Одеська морська академія»
кандидат політичних наук, доцент
ORCID: *https://orcid.org/0000-0001-5837-6201*

Анотація. У статті досліджено оцінку впливу високоризикових систем штучного інтелекту на права людини як самостійний інструмент правової політики України в умовах євроінтеграції, воєнного стану та інтенсивної цифровізації публічного сектору. Обґрунтовано, що автономні системи озброєння, алгоритмічні інструменти у медицині, правоохоронній діяльності, правосудді, освіті та науці мають спільну ознаку підвищеного ризику: вони здатні впливати на життя, здоров'я, приватність, рівність, справедливий суд, людську автономію та довіру до державних інституцій. Доведено, що традиційна модель постфактум-відповідальності є недостатньою для таких технологій, оскільки шкода від помилкових або дискримінаційних алгоритмічних рішень може мати масовий, прихований, кумулятивний і складно відновлюваний характер. Підкреслено, що правова політика у сфері штучного інтелекту має бути не лише інноваційно орієнтованою, а й превентивною, процедурно прозорою та сумісною з принципами верховенства права. На підставі аналізу AI Act, Рекомендації CM/Rec(2020)1 Комітету Міністрів Ради Європи, позицій ВООЗ, МКЧХ, ЮНЕСКО, СЕРЕЈ, а також українських доктринальних підходів запропоновано розглядати HRIA/FRIA як обов'язкову ex ante-процедуру для високоризикових систем штучного інтелекту у публічному секторі. Така процедура має включати ідентифікацію цілей використання системи, класифікацію ризиків, перевірку якості та походження даних, аналіз впливу на вразливі групи, встановлення меж людського нагляду, аудит, логування, прозорість, механізми пояснення, оскарження та періодичний післявпроваджувальний моніторинг. Додатково акцентовано увагу на необхідності незалежного контролю, фіксації відповідальних суб'єктів і недопущення формального перетворення оцінки впливу на внутрішню адміністративну анкету. Сформульовано пропозиції щодо закріплення оцінки впливу в Концепції розвитку штучного інтелекту в Україні, майбутньому рамковому законі та галузевих актах для оборонної, медичної, правоохоронної, судової й освітньої сфер.

Ключові слова: штучний інтелект, високоризикові системи, права людини, HRIA, FRIA, AI Act, правова політика, євроінтеграція, людський нагляд, попереджувальний конституціоналізм.

e-ISSN: 2786-586X

АКАДЕМІЧНІ ВІЗІЇ
Випуск 55/2026

HUMAN RIGHTS IMPACT ASSESSMENT OF HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS AS AN INSTRUMENT OF UKRAINE'S LEGAL POLICY

Vladyslav Oleksiyovych VARYNSKYI
Associate Professor at the Department of Philosophy and Ukrainian Studies, National University "Odesa Maritime Academy"
Candidate of Political Sciences, Associate Professor
ORCID: https://orcid.org/0000-0001-5837-6201

Abstract. The article examines the assessment of the impact of high-risk artificial intelligence systems on human rights as an independent instrument of Ukraine's legal policy in the context of European integration, martial law and intensive digitalization of the public sector. It is substantiated that autonomous weapons systems, algorithmic tools in medicine, law enforcement, justice, education and science have a common feature of increased risk: they are capable of affecting life, health, privacy, equality, fair trial, human autonomy and trust in state institutions. It is proven that the traditional model of post-factum liability is insufficient for such technologies, since the damage from erroneous or discriminatory algorithmic decisions can be massive, hidden, cumulative and difficult to restore. It is emphasized that legal policy in the field of artificial intelligence should be not only innovation-oriented, but also preventive, procedurally transparent and compatible with the principles of the rule of law. Based on the analysis of the AI Act, Recommendation CM/Rec(2020)1 of the Committee of Ministers of the Council of Europe, the positions of the WHO, ICRC, UNESCO, CEPEJ, as well as Ukrainian doctrinal approaches, it is proposed to consider HRIA/FRIA as a mandatory ex ante procedure for high-risk artificial intelligence systems in the public sector. Such a procedure should include identification of the purposes of using the system, classification of risks, verification of the quality and origin of data, analysis of the impact on vulnerable groups, establishment of limits of human supervision, audit, logging, transparency, mechanisms of explanation, appeal and periodic post-implementation monitoring. In addition, attention is focused on the need for independent control, fixing of responsible entities and preventing the formal transformation of the impact assessment into an internal administrative questionnaire. Proposals are formulated to consolidate the impact assessment in the Concept of the Development of Artificial Intelligence in Ukraine, the future framework law and sectoral acts for the defense, medical, law enforcement, judicial and educational spheres.

Keywords: artificial intelligence, high-risk systems, human rights, HRIA, FRIA, AI Act, legal policy, European integration, human oversight, preventive constitutionalism.

Актуальність. Розвиток систем штучного інтелекту поступово переводить цифровізацію публічного сектору з площини технічної модернізації у площину конституційно значущого правового регулювання. Якщо традиційні інформаційні системи переважно забезпечували зберігання, пошук або передання даних, то сучасні алгоритмічні моделі здатні самостійно виявляти закономірності, формувати рекомендації, оцінювати ризики, ранжувати осіб, прогнозувати поведінку, підтримувати або фактично визначати владні рішення. Саме ця здатність до навчання на даних, адаптації та впливу на юридично значущі наслідки відрізняє штучний інтелект від звичайних автоматизованих систем і зумовлює потребу в особливому режимі правового контролю [5; 6].

e-ISSN: 2786-586X

Найбільш проблемними є ті сфери, де алгоритмічне рішення або рекомендація стосується життя, здоров'я, фізичної безпеки, приватності, рівності, свободи пересування, права на справедливий суд, доступу до освіти чи довіри до держави. До таких сфер належать автономні системи озброєння, медичні системи підтримки клінічних рішень, правоохоронні аналітичні інструменти, системи біометричної ідентифікації, алгоритмічна підтримка судочинства, освітні платформи та засоби автоматизованого оцінювання. Їх об'єднує не тотожність технологічного призначення, а підвищена інтенсивність впливу на основоположні права людини.

У такому контексті юридична проблема полягає не лише в тому, щоб визначити, які системи штучного інтелекту можуть бути дозволені, обмежені або заборонені. Більш фундаментальним є питання: яким чином держава має оцінювати ризики таких систем до моменту їх впровадження, хто повинен відповідати за таку оцінку, які права та інтереси мають бути перевірені, як забезпечити участь зацікавлених сторін і як перетворити результати оцінки на юридично значущі умови використання технології. Саме тому оцінка впливу на права людини та основоположні права (HRIA/FRIA) має розглядатися не як факультативна етична процедура, а як обов'язковий елемент ризико-орієнтованої правової політики України у сфері штучного інтелекту.

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання цифрових технологій і штучного інтелекту в українській доктрині розвивається на перетині інформаційного, адміністративного, конституційного, кримінального, медичного та освітнього права. О. Баранов обґрунтовує необхідність теоретико-методологічного осмислення правового регулювання Інтернету речей і пов'язаних із ним ризиків, що є важливим для розуміння інфраструктурного середовища штучного інтелекту [12]. Н. Савінова аналізує кримінально-правову політику убезпечення інформаційного суспільства, акцентуючи на необхідності превентивного реагування на інформаційно-технологічні ризики [13; 14]. К. Некіт розглядає правові проблеми Інтернету речей, які прямо корелюють із питаннями відповідальності, даних і контролю над автономізованими технічними системами [15].

Міжнародний і європейський вимір дослідження формують документи Ради Європи, Європейського Союзу, ВООЗ, МКЧХ, ЮНЕСКО та СЕРЕЇ. Рекомендація CM/Rec(2020)1 закріплює необхідність оцінки впливу алгоритмічних систем на права людини, прозорості, недискримінації, підзвітності та людського контролю [2]. AI Act розвиває цю логіку через класифікацію систем штучного інтелекту за рівнями ризику, запровадження вимог до високоризикових систем, технічної документації, людського нагляду, післяринкового моніторингу та оцінки впливу на основоположні права [1]. ВООЗ формулює етичні принципи використання штучного інтелекту у сфері охорони здоров'я [7], МКЧХ і ООН порушують питання автономних систем озброєння та необхідності meaningful human control [8; 9; 10], а СЕРЕЇ і ЮНЕСКО акцентують на ризиках штучного інтелекту для судової незалежності, справедливого суду та верховенства права [17; 18].

Попри значний масив джерел, у національній правовій доктрині ще недостатньо розроблено цілісну модель оцінки впливу високоризикових систем штучного інтелекту на права людини як інструменту правової політики. Здебільшого аналіз ведеться або навколо окремих секторів, або навколо загальних принципів регулювання. Натомість потребує конкретизації саме міжсекторальна процедура HRIA/FRIA, здатна поєднати європейську risk-based модель із українським безпековим, інституційним і правозахисним контекстом.

e-ISSN: 2786-586X

Метою статті є формування науково обґрунтованої моделі оцінки впливу високоризикових систем штучного інтелекту на права людини як інструменту правової політики України з урахуванням європейського ризико-орієнтованого підходу, специфіки воєнного стану та потреби нормативного врегулювання використання штучного інтелекту в оборонній, медичній, правоохоронній, судовій та освітній сферах.

Виклад основгого матеріалу. Ризико-орієнтована модель регулювання штучного інтелекту виходить із того, що інтенсивність правових обмежень має залежати не від технологічної новизни системи як такої, а від потенційної шкоди, яку вона здатна завдати правам людини, демократії, публічній безпеці та верховенству права. Такий підхід відрізняється від двох крайніх моделей: повної технологічної лібералізації, яка залишає ризики на розсуд розробників і користувачів, та тотальної заборони, що блокує суспільно корисні інновації. Його зміст полягає у градації застосувань: неприйнятні практики мають заборонятися, високоризикові системи - допускатися лише за умов спеціальних гарантій, а низькоризикові інструменти - функціонувати за пом'якшеними правилами.

AI Act закріплює саме таку логіку, поєднуючи заборону окремих практик, спеціальний режим для високоризикових систем, вимоги до прозорості та механізми нагляду [1]. Рекомендація CM/Rec(2020)1 Ради Європи методологічно передувала цій моделі, оскільки вже у 2020 р. запропонувала розглядати алгоритмічні системи крізь призму впливу на права людини, пропорційності втручання, прозорості, недискримінації, захисту даних, підзвітності й оцінки ризиків до впровадження [2]. Для України ці документи мають не лише порівняльне, а й програмне значення, оскільки євроінтеграційний курс вимагає наближення національного регулювання до acquis ЄС, а воєнний стан потребує додаткових запобіжників від надмірної сек'юритизації цифрових інструментів.

У межах високоризикових сфер можна виокремити три критерії, які обґрунтовують необхідність обов'язкової оцінки впливу. Перший критерій - безпосередній вплив на життя, здоров'я, тілесну недоторканність і фізичну безпеку. Він найбільш виразно проявляється в автономних системах озброєння, медичних алгоритмах і частині правоохоронних застосувань. Другий критерій - вплив на процесуальні гарантії, справедливий суд, презумпцію невинуватості та правовий статус особи; він характерний для правоохоронної аналітики, судових систем підтримки рішень і алгоритмів оцінки ризику. Третій критерій - довгостроковий вплив на формування людського капіталу, освітні траєкторії, академічну доброчесність і здатність особи до автономного мислення; він стосується освітніх та наукових застосувань штучного інтелекту.

HRIA/FRIA як ex ante-механізм правового контролю. Оцінка впливу на права людини та основоположні права повинна передувати впровадженню високоризикової системи штучного інтелекту. Її призначення полягає не в легітимації вже прийнятого технологічного рішення, а у перевірці того, чи є таке рішення юридично допустимим, пропорційним, необхідним у демократичному суспільстві та сумісним із ядром прав людини. У цьому сенсі HRIA/FRIA є проявом попереджувального конституціоналізму: держава перевіряє цифрову систему не після порушення права, а до того, як система почне впливати на особу або групу осіб.

На відміну від класичної оцінки технічної безпеки, HRIA/FRIA має охоплювати не лише надійність, кіберзахист або точність алгоритму, а й соціально-правові наслідки його використання. Для цього необхідно встановити легітимну мету застосування системи, характер даних, що використовуються для навчання та функціонування моделі,

e-ISSN: 2786-586X

можливість виникнення дискримінаційних результатів, ступінь пояснюваності, роль людини в ухваленні остаточного рішення, коло осіб, на яких впливає система, а також процедури оскарження, аудиту та моніторингу. Саме такий підхід дозволяє перевести дискусію про штучний інтелект із площини загальної етики у площину юридично перевірюваних критеріїв.

Для публічного сектору HRIA/FRIA має бути обов'язковою не лише щодо систем, які безпосередньо ухвалюють рішення, а й щодо систем, які формують рекомендації, рейтинги, профілі, індикатори ризику або попередні висновки для посадової особи. Формально людина може залишатися суб'єктом остаточного рішення, однак за наявності automation bias алгоритмічний висновок здатний фактично визначати зміст людського розсуду. Тому людський нагляд має бути змістовним, а не номінальним: оператор повинен мати повноваження, час, компетентність і фактичну можливість не погодитися з рекомендацією системи.

Секторальне значення оцінки впливу. В оборонній сфері оцінка впливу штучного інтелекту має враховувати вимоги міжнародного гуманітарного права, принципи розрізнення, пропорційності, запобігання надмірним стражданням і збереження людського контролю над критичними функціями вибору та ураження цілей. МКЧХ пов'язує автономні системи озброєння саме з можливістю самостійного вибору й атаки цілей, що вимагає спеціального правового режиму [8]. Резолюції Генеральної Асамблеї ООН щодо летальних автономних систем озброєння підтверджують, що проблема вже вийшла за межі технічної дискусії і стала питанням міжнародної безпеки, відповідальності та гуманітарного права [9; 10]. Для України, яка перебуває в умовах збройної агресії, це означає потребу поєднати оборонну інноваційність із недопущенням повної делегації летального рішення машині.

У медичній сфері HRIA/FRIA має бути доповнена оцінкою клінічної безпеки, інформованої згоди, якості медичних даних, впливу на лікарську автономію та недискримінаційного доступу до лікування. ВООЗ визначає ключовими принципами автономію людини, добробут і безпеку, прозорість, відповідальність, інклюзивність і сталість штучного інтелекту [7]. Отже, медичний алгоритм не може розглядатися лише як програмний продукт: він є елементом медичного втручання або клінічного процесу, здатним впливати на діагноз, лікування, пріоритетність доступу до ресурсів та довіру пацієнта до системи охорони здоров'я.

У правоохоронній діяльності та сфері публічної безпеки оцінка впливу повинна охоплювати ризики масового спостереження, біометричної ідентифікації, предиктивної аналітики, алгоритмічного профілювання та селективного застосування владних повноважень. Особливе значення має перевірка того, чи не перетворює система статистичну кореляцію на підставу для посиленого контролю над особою, яка не вчинила правопорушення. У цьому контексті HRIA/FRIA має встановлювати межі допустимого використання даних, заборону прихованого або неконтрольованого масового спостереження, обов'язковість логування дій системи й можливість незалежної перевірки її результатів.

У правосудді штучний інтелект може використовуватися для пошуку практики, аналізу документів, структурування доказової інформації, прогнозування навантаження або допоміжного аналізу правових позицій. Однак він не повинен підміняти суддівський розсуд, обов'язок мотивувати рішення та гарантії справедливого суду. Європейська етична хартія CEPEJ щодо використання штучного інтелекту у судових системах виходить

e-ISSN: 2786-586X

із пріоритету фундаментальних прав, недискримінації, якості, безпеки, прозорості й контролю користувача [17]. Відповідно, HRIA/FRIA у судовій сфері має перевіряти не лише технічну коректність інструмента, а й його вплив на незалежність суду, рівність сторін і право особи зрозуміти мотиви рішення.

В освіті та науці високоризиковий характер мають системи автоматизованого оцінювання, академічного моніторингу, виявлення недоброчесності, адаптивного навчання та аналітики поведінки здобувачів. Їхній вплив не завжди є миттєвим, але може бути кумулятивним: алгоритм здатний формувати освітню траєкторію, впливати на самооцінку здобувача, посилювати нерівність доступу до якісної освіти або створювати надмірний цифровий контроль. Тому оцінка впливу в цій сфері має включати аналіз педагогічної доцільності, недискримінаційності, захисту персональних даних, академічної доброчесності та збереження ролі викладача як суб'єкта освітнього процесу.

Національна модель впровадження HRIA/FRIA. Для України доцільно закріпити багаторівневу модель оцінки впливу високоризикових систем штучного інтелекту. На концептуальному рівні відповідні положення мають бути внесені до Концепції розвитку штучного інтелекту в Україні, яка повинна не лише підтримувати інновації, а й прямо визначати обмеження, права людини, ризико-орієнтовану класифікацію та обов'язковість попередньої оцінки для публічного сектору [3; 4]. На програмному рівні Біла книга та майбутня стратегія мають бути переорієнтовані з переважно добровільної моделі на диференційовану модель: там, де ризик є мінімальним, допустимими можуть бути рекомендаційні інструменти, але у високоризикових сферах потрібне обов'язкове регулювання [16].

На законодавчому рівні майбутній рамковий акт про штучний інтелект повинен передбачити: класифікацію систем за рівнями ризику; перелік неприйнятних практик; загальні вимоги до високоризикових систем; обов'язкову HRIA/FRIA для державних органів і суб'єктів, що виконують публічні функції; процедури незалежного аудиту; вимоги до технічної документації та логування; обов'язок інформування осіб про суттєву алгоритмічну участь; право на пояснення та оскарження; правила післявпроваджувального моніторингу; санкції за порушення режиму використання.

На галузевому рівні мають бути розроблені спеціальні методики оцінки впливу для оборони, медицини, правоохоронної діяльності, правосуддя, освіти та науки. Єдина загальна методика не може однаково ефективно охопити ризики автономної зброї, медичного діагностичного алгоритму, системи розпізнавання облич, судового аналітичного інструмента і програми автоматизованого оцінювання студентських робіт. Водночас усі секторальні методики повинні містити спільне ядро: права, на які впливає система; легітимна мета; пропорційність; якість і походження даних; недискримінація; людський нагляд; прозорість; аудит; оскарження; періодичний перегляд.

Окремої уваги потребує інституційна архітектура. Оцінка впливу не може залишатися внутрішнім документом органу або розробника, якщо йдеться про високоризикові публічні застосування. Потрібні незалежний нагляд, залучення Уповноваженого Верховної Ради України з прав людини, органу із захисту персональних даних, профільних міністерств, експертного середовища, громадських організацій і професійних спільнот. У найбільш чутливих випадках, зокрема щодо біометричного спостереження, правоохоронного профілювання або судових алгоритмів, має бути передбачений судовий або квазісудовий контроль до початку експлуатації системи.

e-ISSN: 2786-586X

Воєнний стан не скасовує необхідності HRIA/FRIA, а змінює акценти її проведення. Частина обмежень може адаптуватися до потреб оборони, контррозвідки або документування воєнних злочинів, однак така адаптація має бути тимчасовою, цільовою, пропорційною та підконтрольною. Найбільша небезпека полягає в тому, що надзвичайні алгоритмічні інструменти, виправдані війною, можуть бути інституціоналізовані як звичайна практика після завершення воєнного стану. Тому HRIA/FRIA має включати sunset-критерії, періодичний перегляд, обмеження строків зберігання даних і спеціальний аудит воєнних застосувань штучного інтелекту.

З урахуванням європейських стандартів і українського контексту доцільно запропонувати таку базову структуру HRIA/FRIA для високоризикових систем штучного інтелекту:

- ідентифікація системи, її розробника, користувача, оператора, сфери застосування та легітимної мети;
- визначення рівня ризику з урахуванням сфери застосування, автономності системи, характеру даних і можливих наслідків для особи;
- опис прав людини та публічних інтересів, на які система може впливати, із виділенням особливо вразливих груп;
- оцінка якості, репрезентативності, законності отримання та обмежень навчальних і операційних даних;
- перевірка прозорості, пояснюваності, можливості аудиту, логування та зовнішньої перевірки результатів;
- визначення моделі людського нагляду: human-in-the-loop, human-on-the-loop або інша форма змістовного контролю;
- оцінка ризиків дискримінації, помилкової ідентифікації, автоматизаційного упередження, надмірного стеження або підміни людського розсуду;
- визначення юридичних запобіжників: заборони, обмеження, дозволи, спеціальні процедури, незалежний аудит, судовий контроль, право на пояснення та оскарження;
- публічне або обмежено-публічне оприлюднення результатів оцінки з урахуванням вимог безпеки та захисту чутливої інформації;
- післявпроваджувальний моніторинг, звітування про інциденти, періодичний перегляд і можливість зупинення системи.

Запропонована процедура не повинна перетворюватися на формальну бюрократичну анкету. Її правова цінність полягає в тому, що вона створює доказовий ланцюг відповідальності: від рішення про розроблення або закупівлю системи до її експлуатації, аудиту, перегляду й можливого припинення використання. Саме такий ланцюг дає змогу уникнути ситуації, коли шкода від алгоритмічного рішення виявляється, але неможливо встановити, хто саме відповідає за якість даних, параметри моделі, межі людського контролю або правомірність використання системи.

Висновки. Високоризикові системи штучного інтелекту у сферах оборони, медицини, правоохоронної діяльності, правосуддя, освіти та науки потребують не лише загального нормативного регулювання, а й спеціального механізму попередньої оцінки впливу на права людини. Їхній ризик визначається не технологічною складністю самою по собі, а здатністю впливати на життя, здоров’я, приватність, рівність, справедливий суд, людську автономію та довіру до держави.

HRIA/FRIA має бути інституціоналізована в Україні як обов’язкова ex ante-процедура для високоризикових систем штучного інтелекту в публічному секторі та у

e-ISSN: 2786-586X

сферах, де приватні суб'єкти виконують суспільно значущі або делеговані функції. Така процедура повинна поєднувати технічну оцінку, правозахисний аналіз, перевірку пропорційності, аудит даних, аналіз дискримінаційних наслідків, визначення моделі людського нагляду, логування, оскарження та післявпроваджувальний моніторинг.

Українська модель регулювання штучного інтелекту має враховувати AI Act і CM/Rec(2020)1, однак не може бути механічним копіюванням європейських рішень. Вона повинна адаптувати risk-based підхід до умов воєнного стану, гібридних загроз, цифровізації публічного управління, потреб оборони та обмеженої інституційної спроможності окремих органів.

На нормативному рівні доцільно закріпити HRIA/FRIA у Концепції розвитку штучного інтелекту в Україні, майбутньому рамковому законі про штучний інтелект і спеціальних галузевих актах. Особливої уваги потребують автономні системи озброєння, медичні алгоритми, правоохоронні системи спостереження й профілювання, судові аналітичні інструменти та освітні системи автоматизованого оцінювання.

Подальші дослідження мають бути спрямовані на розроблення типових методик HRIA/FRIA для окремих секторів, визначення компетентного органу або мережі органів нагляду, встановлення стандартів незалежного аудиту та формування процесуальних гарантій оскарження результатів алгоритмічної участі у владних рішеннях.

Список використаних джерел

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024.
2. Рекомендація CM/Rec(2020)1 Комітету Міністрів Ради Європи державам-членам щодо впливу алгоритмічних систем на права людини: ухвалена 8 квітня 2020 р. URL: https://www.nrada.gov.ua/wp-content/uploads/2020/05/Rec-20201-UKR.pdf
3. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220
4. Біла книга з регулювання ШІ в Україні: бачення Мінцифри / уклад. Г. Румянцев. Міністерство цифрової трансформації України, 2024.
5. Brynjolfsson E., McAfee A. The Business of Artificial Intelligence. Harvard Business Review, 2017. URL: https://starlab-alliance.com/wp-content/uploads/2017/09/AI-Article.pdf
6. Rigano C. Using Artificial Intelligence to Address Criminal Justice Needs. National Institute of Justice, 2018. URL: https://www.ojp.gov/pdffiles1/nij/252038.pdf
7. WHO issues first global report on Artificial Intelligence (AI) in health and six guiding principles for its design and use. World Health Organization, 2021. URL: https://www.who.int/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guiding-principles-for-its-design-and-use
8. Autonomous weapon systems: technical, military, legal and humanitarian aspects. Expert meeting report. International Committee of the Red Cross, Geneva, 2014. URL: https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014
9. United Nations General Assembly. Lethal Autonomous Weapons Systems. Resolution 78/241, 22 December 2023. URL: https://digitallibrary.un.org/record/4033027

e-ISSN: 2786-586X

10. United Nations General Assembly. Lethal Autonomous Weapons Systems. Resolution 79/77, 2 December 2024. URL: https://digitallibrary.un.org/record/4071100
11. Меликов Р. Г. Застосування автономних систем озброєння під час російсько-української війни: нові виклики міжнародному гуманітарному праву. Юридичний науковий електронний журнал. 2023. № 1. С. 620-622. URL: http://lsej.org.ua/1_2023/145.pdf
12. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія. Київ: ДНУ «НДІ інформації, безпеки і права НАПрН України»; Видавничий дім «АрТЕк», 2018. 342 с.
13. Савінова Н. А. Кримінально-правова політика та убезпечення інформаційного суспільства в Україні: монографія. Київ: Редакція журналу «Право України»; Харків: Право, 2013. 289 с.
14. Савінова Н. А. Удосконалення кримінально-правового забезпечення розвитку інформаційного суспільства в Україні. Інформація і право. 2020. № 3. С. 110-140.
15. Некіт К. Г. Деякі правові проблеми інтернету речей і напрями їх вирішення. Часопис цивілістики. 2019. № 31. С. 68-73.
16. Fundamental Rights Agency. Assessing high-risk AI. European Union Agency for Fundamental Rights, 2025. URL: https://fra.europa.eu/en/publication/2025/assessing-high-risk-ai
17. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Strasbourg, 2018.
18. UNESCO. AI and the Rule of Law for the Judiciary. Paris: UNESCO, 2023. URL: https://unesdoc.unesco.org/ark:/48223/pf0000387331
19. Commission Nationale de l'Informatique et des Libertés (CNIL). AI System Development: CNIL's Recommendations to Comply with the GDPR. CNIL, 2024. URL: https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd

References

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024.
2. Recommendation CM/Rec(2020)1 of the Committee of Ministers of the Council of Europe to member states on the impact of algorithmic systems on human rights: adopted on 8 April 2020. URL: https://www.nrada.gov.ua/wp-content/uploads/2020/05/Rec-20201-UKR.pdf
3. On the approval of the Concept of the Development of Artificial Intelligence in Ukraine: Order of the Cabinet of Ministers of Ukraine dated 02.12.2020 No. 1556-p. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220
4. White Paper on Regulation of AI in Ukraine: Vision of the Ministry of Digitalization / Compiled by G. Rumyantsev. Ministry of Digital Transformation of Ukraine, 2024.
5. Brynjolfsson E., McAfee A. The Business of Artificial Intelligence. Harvard Business Review, 2017. URL: https://starlab-alliance.com/wp-content/uploads/2017/09/AI-Article.pdf
6. Rigano C. Using Artificial Intelligence to Address Criminal Justice Needs. National Institute of Justice, 2018. URL: https://www.ojp.gov/pdffiles1/nij/252038.pdf

e-ISSN: 2786-586X

7. WHO issues first global report on Artificial Intelligence (AI) in health and six guiding principles for its design and use. World Health Organization, 2021. URL: https://www.who.int/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guiding-principles-for-its-design-and-use
8. Autonomous weapon systems: technical, military, legal and humanitarian aspects. Expert meeting report. International Committee of the Red Cross, Geneva, 2014. URL: https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014
9. United Nations General Assembly. Lethal Autonomous Weapons Systems. Resolution 78/241, 22 December 2023. URL: https://digitallibrary.un.org/record/4033027
10. United Nations General Assembly. Lethal Autonomous Weapons Systems. Resolution 79/77, 2 December 2024. URL: https://digitallibrary.un.org/record/4071100
11. Melikov R. G. The use of autonomous weapons systems during the Russian-Ukrainian war: new challenges to international humanitarian law. Legal Scientific Electronic Journal. 2023. No. 1. P. 620-622. URL: http://lsej.org.ua/1_2023/145.pdf
12. Baranov O. A. The Internet of Things: theoretical and methodological foundations of legal regulation. Vol. 1: Areas of application, risks and barriers, problems of legal regulation: monograph. Kyiv: DNU "Research Institute of Information, Security and Law of the National Academy of Sciences of Ukraine"; Publishing House "ArTEk", 2018. 342 p.
13. Savinova N. A. Criminal and legal policy and securing the information society in Ukraine: monograph. Kyiv: Editorial Board of the journal "Law of Ukraine"; Kharkiv: Law, 2013. 289 p.
14. Savinova N. A. Improving criminal and legal support for the development of the information society in Ukraine. Information and Law. 2020. No. 3. P. 110-140.
15. Nekit K. G. Some legal problems of the Internet of Things and directions for their solution. Journal of Civil Studies. 2019. No. 31. P. 68-73.
16. Fundamental Rights Agency. Assessing high-risk AI. European Union Agency for Fundamental Rights, 2025. URL: https://fra.europa.eu/en/publication/2025/assessing-high-risk-ai
17. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Strasbourg, 2018.
18. UNESCO. AI and the Rule of Law for the Judiciary. Paris: UNESCO, 2023. URL: https://unesdoc.unesco.org/ark:/48223/pf0000387331
19. Commission Nationale de l'Informatique et des Libertés (CNIL). AI System Development: CNIL's Recommendations to Comply with the GDPR. CNIL, 2024. URL: https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd

e-ISSN: 2786-586X