УДК 342.7:004.056:004.8
DOI 10.32755/sjlaw.2026.103

Покришень Д. А.,
кандидат педагогічних наук, доцент,
директор Навчально-наукового інституту права,
правоохоронної діяльності та психології,
Пенітенціарна академія України,
м. Чернігів, Україна
ORCID: 0000-0001-9572-413X

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ: СИСТЕМНІСТЬ, ВИКЛИКИ ТА ЄВРОІНТЕГРАЦІЙНІ ОРІЄНТИРИ

Здійснено комплексний аналіз нормативно-правового забезпечення кібербезпеки та ШІ в Україні як взаємопов'язаних складових сучасної цифрової екосистеми держави. Досліджено систему нормативних документів, що регламентують захист інформаційного простору, критичної інфраструктури та використання інтелектуальних технологій. Визначено ключові проблеми фрагментарності правового регулювання, ризик-орієнтованого підходу та відповідальності за автономні системи ШІ.

Ключові слова: *кібербезпека, штучний інтелект, інформаційне право, критична інфраструктура, європейські стандарти, правове регулювання.*

Постановка проблеми. Розвиток інформаційного суспільства та інтенсивне впровадження цифрових технологій зумовили якісно новий рівень викликів, що виходять за межі традиційного регулювання інформаційних відносин. Якщо Закон України «Про інформацію» формує базові принципи обігу інформації, гарантує права доступу та визначає загальні вимоги до інформаційної діяльності, то законодавство про кібербезпеку спрямоване на забезпечення захисту цієї інформації від комплексних техногенних та навмисних загроз, що виникають у кіберпросторі. Таким чином, нормативне регулювання кібербезпеки постає як функціональне продовження та поглиблення інформаційно-правових засад, адже ефективна реалізація інформаційних прав неможлива без гарантованого рівня кіберзахисту, стійкості критичної інфраструктури та узгодженої діяльності суб'єктів національної системи безпеки у цифровому середовищі.

Аналіз останніх досліджень і публікацій. У дослідженні Ірини Сопілки [1, с. 110] звернено увагу на те, що система кібербезпеки становить собою багатокомпонентний комплекс, ефективність якого визначається узгодженістю функціонування всіх його елементів у межах організації. До ключових складових такої системи належать: безпека програмного забезпечення, захист даних, забезпечення стійкості критично важливої інфраструктури, мережева та операційна безпека, засоби хмарного захисту, механізми аварійного відновлення та підтримання безперервності бізнес-процесів, фізична безпека, а також систематична підготовка користувачів. У зв'язку з постійною еволюцією кіберзагроз виникає потреба у запровадженні більш динамічних, адаптивних і превентивних підходів, що виходять за межі традиційних моделей захисту, орієнтованих лише на основні компоненти інформаційних систем, і недостатньо враховують уразливість допоміжних.

У роботі Завгородньої Ю. В. [2, с. 33] йдеться, що у сучасних умовах провідні держави світу приділяють особливу увагу захисту власного інформаційного простору, що зумовлено зростанням ролі кіберсфери в системі національної безпеки. Досвід прогресивних країн, які претендують на статус глобальних центрів управління, свідчить про трансформацію військових інструментів державного управління та активне формування спеціалізованих кіберпідрозділів.

У дослідженні Покришня Д. А. [3, с. 56] розглядаються конкретні кейси використання систем генеративного штучного інтелекту, що демонструє сучасний стан можливостей ШІ.

Метою статті є комплексний аналіз нормативно-правових засад забезпечення кібербезпеки та регулювання штучного інтелекту в Україні, виявлення системних проблем і прогалин правового регулювання, а також обґрунтування напрямів його вдосконалення з урахуванням європейських стандартів, міжнародних практик і потреб національної безпеки в умовах цифрової трансформації.

Виклад основного матеріалу. Нормативно-правове регулювання кібербезпеки в Україні сформувалося як багаторівнева, комплексна та адаптивна система, яка відображає сучасні загро-

зи й потреби захисту державних інформаційних ресурсів і критичної інфраструктури. Воно поєднує рамкові положення законів, стратегічні засади державної політики та детальні технічні регламенти підзаконного рівня, що забезпечує системність і узгодженість механізмів протидії кіберзагрозам. Центральним елементом цієї системи є Закон України «Про основні засади забезпечення кібербезпеки України», який відіграє роль концептуального ядра, визначає структуру національної системи кібербезпеки, окреслює принципи захисту інформаційного простору та регламентує взаємодію суб'єктів у межах єдиного координаційного механізму. У взаємозв'язку з ним діють положення законів «Про національну безпеку України» та «Про критичну інфраструктуру», що доповнюють фундаментальні підходи до забезпечення захисту ключових секторів економіки і визначають особливий режим управління кіберризиками.

Стратегічний рівень нормативного регулювання створюється за рахунок Стратегії кібербезпеки України та рішень Ради національної безпеки і оборони, які визначають довгострокові орієнтири державної політики, враховують зміни у характері кібератак, технологічні тренди та загрозливі тенденції міжнародного середовища. Укази Президента та рішення РНБО спрямовані на оперативне реагування на комплексні кіберінциденти, підвищення рівня готовності державних органів до реагування на масштабні кібератаки та реалізацію політики стримування у кіберпросторі. Таким чином, стратегічні документи формують концептуальний каркас безпеки, що забезпечує функціональну взаємодію всіх суб'єктів Національної системи кібербезпеки, включно із СБУ, Держспецзв'язку, Національним координаційним центром кібербезпеки при РНБО, Національною поліцією та іншими інституціями.

Підзаконний рівень, представлений постановами Кабінету Міністрів України та наказами Державної служби спеціального зв'язку та захисту інформації, забезпечує деталізацію технічних, організаційних і процедурних вимог, необхідних для практичного функціонування систем кіберзахисту. Зокрема, нормативно визначаються вимоги до створення, атестації та аудиту систем захисту об'єктів критичної інфраструктури, порядок ви-

явлення та реагування на вразливості, а також регламенти оцінювання стану захищеності державних інформаційних ресурсів. У цих документах зосереджено акцент на стандартизації технічних заходів, впровадженні сучасних моделей управління ризиками та забезпеченні інтегрованого підходу до захисту інформаційних систем.

Однією зі специфічних особливостей українського кібербезпекового законодавства є його підвищена орієнтованість на захист об'єктів критичної інфраструктури. Зростання кількості цілеспрямованих кібератак на енергетичний сектор, транспортні та комунікаційні системи, фінансові інституції та адміністративні ресурси зумовило формування нормативних вимог щодо обов'язковості впровадження механізмів кіберзахисту для таких суб'єктів. Вимоги до оцінювання ризиків, створення систем оперативного реагування, проведення аудиту кіберзахисту та реалізації процедур кіберстійкості орієнтовані на мінімізацію впливу можливих атак на функціонування держави та забезпечення безперервності критичних процесів. Таким чином, захист критичної інфраструктури став пріоритетом державної політики, що відповідає світовим тенденціям і рекомендаціям міжнародних організацій.

Ще однією важливою рисою національної нормативної бази є вагома роль Державної служби спеціального зв'язку та захисту інформації, а також створеної на її базі команди реагування на комп'ютерні надзвичайні події CERT-UA. Саме ці органи відіграють ключову роль в оперативній протидії кіберінцидентам, моніторингу кіберпростору, координації взаємодії між суб'єктами кібербезпеки та впровадженні технічних стандартів захисту. Їхня діяльність спрямована на запобігання масштабним загрозам, локалізацію кібератак, забезпечення обміну інформацією та формування національної системи раннього попередження.

Суттєвою тенденцією останніх років є перехід України від формальних, переважно нормативно-зарегульованих підходів до створення комплексних систем захисту інформації до сучасної ризик-орієнтованої моделі, що відображає принципи міжнародних стандартів, включно з ISO 27001 та директивами NIS/NIS2 ЄС. Такий підхід сприяє підвищенню ефективності кіберзахис-

ту, оскільки дає змогу гнучко адаптувати системи безпеки до конкретних загроз, оптимізувати витрати та забезпечувати реальну, а не формальну кіберстійкість.

Узагальнюючи, нормативна база кібербезпеки в Україні становить багатокомпонентну та структурно інтегровану систему, яка поєднує правові, організаційні й технічні механізми забезпечення захисту державних інтересів у кіберпросторі. Її розвиток визначається поєднанням міжнародних стандартів, потреб національної безпеки та викликів цифрової трансформації, а ключовим пріоритетом залишається підвищення кіберстійкості критичної інфраструктури, розбудова ефективної моделі міжвідомчої взаємодії та створення умов для оперативного реагування на кіберзагрози. Така системність і адаптивність дозволяють розглядати національне кібербезпекове законодавство як важливий чинник посилення обороноздатності держави та її інтеграції до європейського кіберпростору.

Розгляд нормативно-правового забезпечення кібербезпеки створює ґрунтовні передумови для переходу до аналізу правового регулювання штучного інтелекту, оскільки обидві сфери є складовими сучасної цифрової екосистеми держави та взаємопов'язані за своїм змістом і стратегічними цілями. Якщо законодавство про кібербезпеку формує інституційні та технічні механізми захисту інформаційних ресурсів і критичної інфраструктури від кіберзагроз, то нормативна база щодо штучного інтелекту окреслює напрями розвитку технологій, які функціонують у межах цього захищеного середовища та водночас породжують нові типи ризиків, пов'язаних з автономністю рішень, обробкою великих масивів даних і етичними аспектами алгоритмічного управління. Таким чином, дослідження правового регулювання ШІ логічно продовжує аналіз кібербезпекових норм, адже від рівня захищеності цифрової інфраструктури та зрілості національної системи кіберзахисту безпосередньо залежить можливість безпечного, контрольованого та відповідального впровадження інтелектуальних технологій у різні сфери суспільного життя.

Проведений аналіз Габані І. [4, с. 112] теоретичних і практичних аспектів використання міжнародної інформації у право-

застосуванні засвідчує, що поєднання транскордонних інформаційних ресурсів з технологіями штучного інтелекту створює значний потенціал для підвищення ефективності боротьби з транснаціональною злочинністю, зокрема шляхом автоматизованої аналітики великих масивів даних, прогнозування злочинних дій та ідентифікації підозрюваних, що вже реалізується у таких системах, як I-24/7 INTERPOL та EIS EUROPOL. Водночас упровадження ШІ супроводжується низкою правових та етичних ризиків, пов'язаних із захистом приватності, алгоритмічною упередженістю та необхідністю забезпечення правомірності транскордонного обміну даними, що знаходить відображення у положеннях Будапештської конвенції Ради Європи про кіберзлочинність. За цих умов міжнародна інформація повинна розглядатися як стратегічний ресурс із чітко регламентованим доступом, а інтеграція ШІ потребує впровадження комплексних правових гарантій, зокрема незалежного аудиту алгоритмів та механізмів підзвітності, а також розширення міжнародної координації у сферах кібербезпеки, обміну цифровими доказами та протидії злочинному використанню ШІ. Отже, хоча штучний інтелект здатний суттєво посилити аналітичні та превентивні можливості правоохоронних органів у сфері міжнародної взаємодії, ефективність і легітимність його застосування можлива лише за умови дотримання міжнародно-правових стандартів, оновлення нормативної бази, формування спільних етичних принципів і поглиблення глобальної співпраці.

Аналіз окресленої проблематики Ю. Бурилом [5, с. 145] свідчить, що фундаментальна відмінність між традиційними інформаційно-комунікаційними системами та системами, заснованими на штучному інтелекті, полягає в можливості останніх виходити за межі людського контролю завдяки здатності до автономного програмування, самонавчання та прийняття рішень, які не завжди можуть бути передбачені їхніми розробниками. Така перспектива формує суттєвий виклик для права, оскільки історично механізм правового регулювання ґрунтувався на впливі на людину як свідому, раціональну істоту, здатну розуміти юридичні приписи та коригувати свою поведінку. У традиційній моделі саме людина виступає суб'єктом правовідносин

і через власні дії опосередковує вплив права на інформаційні системи. Проте поява автономних ШІ-систем ставить під сумнів ефективність такої моделі, адже у разі зростання їхньої ролі у формуванні інформаційних процесів та економічних відносин вони можуть чинити вплив на економічну та інформаційну систему загалом у значно більшому обсязі, ніж людина. Це актуалізує необхідність перегляду підходів до правового регулювання та вироблення нових концепцій відповідальності та контролю у сфері взаємодії між людиною, штучним інтелектом і суспільними відносинами.

Вплив штучного інтелекту на розвиток інформаційного права, як засвідчує дослідження А. Бєгун [6, с. 37], полягає в тому, що одним із ключових викликів є питання достовірності й точності рішень, які ухвалюють ШІ-системи, адже їхні судження ґрунтуються на обробці великих масивів даних і формуванні статистичних узагальнень, що не завжди відображають індивідуальні особливості конкретної особи. Застосування таких систем у процесах прийняття рішень щодо окремих людей створює ризики порушення їхніх прав, особливо в ситуаціях, коли алгоритми базуються на історичних даних, які містять упередження чи елементи дискримінації, що може призводити до хибних та несправедливих висновків. У цих умовах постає необхідність формування належного нормативно-правового регулювання, спрямованого на забезпечення захисту персональних даних, запобігання алгоритмічній дискримінації та встановлення етичних обмежень, які гарантували б збалансоване поєднання інноваційного потенціалу штучного інтелекту з дотриманням фундаментальних прав і свобод людини в цифровому середовищі.

Узагальнення міжнародних тенденцій регулювання штучного інтелекту А. Марущаком [7, с. 55] свідчить, що процеси неминуче мають бути інтегровані в систему інформаційного права України, адже розвиток ШІ безпосередньо впливає на правовий режим інформації, її обіг, безпеку та захист прав суб'єктів інформаційних відносин. Аналіз документів ООН, G7, ЄС, США та Китаю демонструє складність формування уніфікованої глобальної моделі регулювання ШІ, оскільки позиції держав коливаються між необхідністю створення всеосяжної міжнародної

конвенції та побоюваннями надмірного регулювання, яке може стримувати інновації. У цьому контексті особливого значення набуває введення в дію Акта ЄС про штучний інтелект, що формуватиме стандарти, обов'язкові не лише для країн-членів, але й для розробників з інших держав, включно з Україною. Водночас чинні українські нормативні акти у сфері ШІ не повністю відповідають світовим підходам, що актуалізує потребу гармонізації національного законодавства з міжнародними практиками у частині етичності, прозорості, підзвітності та безпеки ШІ-систем. Розроблення спеціального закону про створення й використання ШІ та можливе формування уповноваженого органу з нагляду за ШІ є необхідними кроками для забезпечення правової визначеності та захисту прав людини в умовах стрімкого розвитку цифрових технологій. При цьому важливо врахувати досвід ЄС і США, а також рекомендації Кодексу поведінки для організацій, які розробляють передові ШІ-системи, зокрема щодо внутрішнього й зовнішнього тестування, прозорості функціонування алгоритмів, обміну інформацією та звітування про інциденти, що сприятиме зміцненню інформаційної безпеки та формуванню ефективної моделі правового регулювання ШІ в Україні.

Нормативно-правове регулювання штучного інтелекту в Україні перебуває на стадії становлення та характеризується рамковістю, фрагментарністю і залежністю від суміжних правових інститутів. Відсутність спеціального комплексного закону про штучний інтелект зумовлює те, що правове поле формується переважно на основі стратегічних документів та окремих норм, інтегрованих в акти, які регулюють інтелектуальну власність, захист даних, кібербезпеку та інформаційні відносини. Попри це, наявні нормативні засади вже демонструють прагнення держави до інституціоналізації цієї сфери та до гармонізації національного регулювання з міжнародними та європейськими стандартами.

Центральним документом, який визначає засади державної політики у сфері штучного інтелекту, є Концепція розвитку штучного інтелекту в Україні, затверджена розпорядженням Кабінету Міністрів України 2020 року. Вона визначає стратегічні пріоритети, сфери застосування, ключові напрями стимулювання розвитку та впровадження технологій ШІ, а також окреслює

необхідність комплексної модернізації нормативного середовища. Концепція виступає дорожньою картою для майбутньої законодавчої бази, проте сама по собі не створює юридично зобов'язальних механізмів і слугує скоріше рамковим політичним орієнтиром, ніж інструментом регуляції.

Суттєвим кроком у правовому розвитку стало внесення змін до Закону України «Про авторське право і суміжні права», який запровадив спеціальний режим *sui generis (права особливого роду)* для захисту неоригінальних об'єктів, створених за допомогою комп'ютерних програм, зокрема систем ШІ. Такий підхід є новаторським у міжнародній практиці, оскільки визнає особливу природу алгоритмічно згенерованого продукту й водночас підтверджує, що системи ШІ не можуть набувати статусу автора. Правовласником визначається людина або організація, яка створила чи контролює програму, що генерує контент. Це свідчить про спробу законодавця адаптувати традиційні інститути інтелектуальної власності до реалій автоматизованого та автономного творення результатів інтелектуальної діяльності.

Паралельно розвиток правового поля ШІ відбувається у контексті законодавства про захист персональних даних, оскільки значна частина алгоритмів функціонує на основі масивів персональної інформації. Закон «Про захист персональних даних» встановлює загальні правила обробки даних, що мають безпосереднє значення для навчання моделей ШІ, проте не вирішує низку специфічних питань, пов'язаних з автоматизованими рішеннями, профілюванням та можливими дискримінаційними наслідками обробки великих даних. Аналогічно положення законодавства у сфері кібербезпеки лише опосередковано охоплюють системи ШІ, наголошуючи переважно на технічних вимогах до захисту інформаційних систем.

Україна також долучилася до міжнародних інструментів регулювання, зокрема до Рамкової конвенції Ради Європи щодо штучного інтелекту, яка встановлює етичні, правові та управлінські стандарти використання ШІ у публічному секторі. Це свідчить про намір держави узгодити національну політику із загальноєвропейськими принципами прозорості, підзвітності та безпечності алгоритмічних систем. Враховуючи активні інте-

граційні процеси, можна очікувати подальше наближення українського законодавства до європейської моделі ризик-орієнтованого регулювання, як це передбачено AI Act ЄС.

Особливої уваги в національному правовому полі потребує проблема правової відповідальності за шкоду, завдану автономними системами ШІ. Нині юридична конструкція відповідальності не враховує специфіки алгоритмічної автономності, ступеня впливу людини на функціонування системи, характеру машинного навчання та можливості виникнення помилок, які не можна безпосередньо пов'язати з діями конкретного суб'єкта. Відсутність спеціальної норми створює прогалини у правозастосуванні, що може обмежувати впровадження високорівневих систем ШІ як у державному управлінні, так і в приватному секторі.

Висновки. Таким чином, нормативна база штучного інтелекту в Україні перебуває на етапі становлення й характеризується відсутністю комплексного закону, фрагментарністю регулювання і значною залежністю від загальних норм суміжних правових інститутів. Водночас наявні документи й законодавчі новації демонструють поступове формування юридичного підґрунтя для подальшого розвитку галузі, а орієнтація на європейські стандарти вказує на ймовірний вектор розвитку майбутнього законодавства від декларативних стратегічних орієнтирів до впровадження ризик-орієнтованої, комплексної і практично застосовної моделі регулювання.

Список використаних джерел

1. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 2 (59). С. 110–115. https://doi.org/10.18372/2307-9061.59.15603.

2. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. *Вісник НТУУ "КПІ" Політологія. Соціологія. Право*. 2021. № 4 (52). С. 33–38.

3. Pokryshen D. Artificial Intelligence in education: cases of using ChatGPT 3.5. *Фізико-математична освіта*. 2024. № 1. Т. 39. С. 56–63. https://doi.org/10.31110/fmo2024.v39i1-08.

4. Габані І. І. Міжнародна інформація та штучний інтелект у правозастосувальній діяльності держави. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. № 5 (90). С. 112–116.

5. Бурило Ю. П. Правове регулювання електронного бізнесу: виклики штучного інтелекту. Інноваційна система та інформаційні технології в сучасній науці : матеріали Всеукр. наук.-практ. конф. (м. Харків, м. Київ, 20 жовт. 2017 р.) / редкол.: С. В. Глібко, О. Д. Крупчан, С. А. Бука. Харків : Право, 2017. С. 145–148.

6. Бєгун А. В., Старіна Е. І. Особливості інформаційного права в контексті штучного інтелекту. Моделювання та інформаційні системи в економіці : зб. наук. праць / Київ. нац. екон. ун-т ім. Вадима Гетьмана ; голов. ред. О. Є. Камінський. Київ : КНЕУ, 2023. Вип. 103. С. 37–46. URL: https://ir.kneu.edu.ua/handle/2010/48354.

7. Марущак А. І. Вплив міжнародних процесів регулювання штучного інтелекту на інформаційне право України. *Інформація і право*. 2023. № 4 (47). С. 55–63.

Pokryshen D.,
PhD, Associate Professor, Director of the Educational and Scientific Institute of Law, Law Enforcement Activities and Psychology, Penitentiary Academy of Ukraine, Chernihiv, Ukraine
ORCID: 0000-0001-9572-413X3

LEGAL FRAMEWORK FOR CYBERSECURITY AND ARTIFICIAL INTELLIGENCE IN UKRAINE: SYSTEMIC APPROACH, CHALLENGES AND EUROPEAN INTEGRATION GUIDELINES

The article provides a comprehensive analysis of the legal framework governing cybersecurity and artificial intelligence in Ukraine as interrelated components of the modern digital ecosystem of the state. The study examines legislative and subordinate regulatory acts that define the principles of information security, protection of critical infrastructure, and the development and use of artificial intelligence technologies. It is substantiated that cybersecurity legislation functions as a functional continuation of information law, creating institutional and technical preconditions for the safe implementation of advanced digital solutions.

Special attention is paid to the multi-level structure of cybersecurity regulation, including strategic documents, laws, governmental regulations and technical standards aimed at ensuring cyber resilience and coordinated interagency interaction. The article highlights the growing role of risk-oriented approaches and alignment with international standards, in particular ISO/IEC norms and EU NIS/NIS2 directives.

The legal regulation of artificial intelligence in Ukraine is characterized as fragmented and transitional, largely based on strategic documents and sectoral legislation in the fields of data protection, intellectual property and cybersecurity. The absence of a comprehensive AI law creates legal uncertainty regarding accountability, transparency and control over autonomous systems.

The author concludes that the harmonisation of national legal regulation with European and international standards, the introduction of a risk-based model, and the establishment of clear mechanisms of legal responsibility are essential prerequisites for ensuring secure, ethical and lawful implementation of artificial intelligence technologies within a resilient cybersecurity environment.

Key words: *cybersecurity, artificial intelligence, information law, critical infrastructure, legal regulation, European standards.*

References

1. Sopilko, I. (2021), "Information security and cybersecurity: a comparative-legal aspect", *Scientific Works of Kyiv Aviation Institute. Series: Legal Bulletin "Air and Space Law"*, No. 2 (59), pp. 110–115, DOI: https://doi.org/10.18372/2307-9061.59.15603.

2. Zavgorodnia, Yu. V. (2021), "Cybersecurity as innovative protection in the political space of Ukraine", *Bulletin of NTUU "KPI" Political Science. Sociology. Law*, No. 4 (52), pp. 33–38.

3. Pokryshen, D. (2024), "Artificial Intelligence in education: cases of using ChatGPT 3.5", *Physico-Mathematical Education*, Vol. 39, No. 1, pp. 56–63, DOI: https://doi.org/10.31110/fmo2024.v39i1-08.

4. Habani, I. I. (2025), "International information and artificial intelligence in the law enforcement activities of the state", *Scientific Bulletin of Uzhhorod National University. Series: Law*, No. 5 (90), pp. 112–116.

5. Burylo, Yu. P. (2017), "Legal regulation of electronic business: challenges of artificial intelligence", in Hlibko, S. V., Krupchan, O. D. and Buka, S. A. (Eds.), *Innovative System and Information Technologies in Modern Science* : materials of the All-Ukrainian Scientific-Practical Conference (Kharkiv, Kyiv, 20 October 2017), Kharkiv, Pravo, pp. 145–148.

6. Biegun, A. V. and Starina, E. I. (2023), "Features of information law in the context of artificial intelligence", Modeling and Information Systems in Economics : collection of scientific works, Kyiv National University of Economics named after Vadym Hetman, No. 103, pp. 37–46, available at: https://ir.kneu.edu.ua/handle/2010/48354/.

7. Marushchak, A. I. (2023), "The impact of international AI regulation processes on information law of Ukraine", *Information and Law*, No. 4 (47), pp. 55–63.

Дата першого надходження статті до видання: 02.01.2026.
Дата прийняття статті до друку після рецензування: 17.01.2026.
Дата публікації (оприлюднення): 18.02.2026.