

БІЛОУС Я. В.,

здобувач

*(Науково-дослідний інститут
публічного права)*

УДК 342.9

DOI <https://doi.org/10.32842/2078-3736/2024.2.96>**ПЕРСПЕКТИВНІ НАПРЯМИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ**

Наукова публікація присвячена дослідженню перспективних напрямів удосконалення адміністративно-правового регулювання інформаційних технологій в Україні як необхідної передумови інтеграції держави у глобальний цифровий простір та забезпечення її конкурентоспроможності в умовах цифрової трансформації.

Підкреслюється, що швидкий розвиток інновацій вимагає від України безперервного оновлення та вдосконалення законодавства у сфері інформаційних технологій, так як більшість чинних нормативних документів мають лише декларативний характер або не враховують новітніх технологічних реалій, що ускладнює їхню практичну реалізацію.

Проаналізовано сучасний стан правового забезпечення інформаційних технологій в Україні, виявлено основні прогалини та запропоновано перспективні напрями удосконалення нормативно-правової бази.

Наголошується, що для ефективного використання потенціалу сфери інформаційних технологій необхідне належне адміністративно-правове регулювання, яке відповідатиме європейським та світовим стандартам у сфері захисту персональних даних, сучасним викликам цифрової трансформації та охоплюватиме регулювання новітніх технологій, таких як штучний інтелект, блокчейн та Інтернет речей.

Досліджуються основні виклики України, пов'язані з регулюванням інформаційних технологій, зокрема, гармонізація законодавства України з нормами ЄС, правове регулювання блокчейну, штучного інтелекту та Інтернету речей.

Наголошується на необхідності уніфікації та кодифікації законодавства в сфері інформаційних технологій в Україні як важливого етапу на шляху до побудови розвиненого цифрового суспільства в Україні.

Ключові слова: адміністративно-правове регулювання, інформаційні технології, цифрова трансформація, Загальний регламент захисту даних (GDPR), блокчейн, штучний інтелект, Інтернет речей, Цифровий кодекс України.

Bilous Ya. V. Prospective directions for improving administrative and legal regulation of information technologies in Ukraine

This scientific publication is dedicated to the study of promising directions for improving the administrative and legal regulation of information technologies in Ukraine as a necessary prerequisite for the country's integration into the global digital space and ensuring its competitiveness in the conditions of digital transformation.

It is emphasized that the rapid development of innovations requires Ukraine to continuously update and improve legislation in the field of information technologies, as most existing regulatory documents are merely declarative or do not take into account the latest technological realities, making their practical implementation difficult.



The current state of legal regulation of information technologies in Ukraine is analyzed, key gaps are identified, and prospective directions for improving the regulatory framework are proposed.

It is highlighted that effective utilization of the potential of the information technology sector requires proper administrative and legal regulation that aligns with European and global standards in personal data protection, addresses modern challenges of digital transformation, and covers the regulation of emerging technologies such as artificial intelligence, blockchain, and the Internet of Things.

The study explores Ukraine's key challenges related to the regulation of information technologies, including the harmonization of Ukrainian legislation with EU norms, legal regulation of blockchain, artificial intelligence, and the Internet of Things.

The necessity of unification and codification of legislation in the field of information technologies in Ukraine is emphasized as an important step towards building a developed digital society in the country.

Key words: *administrative and legal regulation, information technologies, digital transformation, General Data Protection Regulation (GDPR), blockchain, artificial intelligence, Internet of Things, Digital Code of Ukraine.*

Вступ. Розвиток цифрових технологій відіграє визначальну роль у сучасному суспільстві, сприяючи економічному зростанню та інтеграції України у світовий інформаційний простір. Проте ефективне використання потенціалу сфери інформаційних технологій неможливе без належного адміністративно-правового регулювання, яке відповідало б сучасним викликам та потребам.

На даний момент в Україні діє низка нормативно-правових актів, що регулюють сферу інформаційних технологій. Однак швидкий розвиток інновацій вимагає безперервного оновлення та вдосконалення законодавства. Деякі існуючі нормативні документи мають декларативний характер або не враховують новітніх технологічних реалій, що ускладнює їхню практичну реалізацію.

Таким чином, дослідження перспективних напрямів удосконалення адміністративно-правового регулювання інформаційних технологій в Україні має як теоретичне, так і практичне значення.

Особливої актуальності вказана тема набуває в контексті євроінтеграційних та глобалізаційних процесів, адже завданням національних органів публічної адміністрації є приведення національного законодавства у відповідність до норм та принципів права ЄС.

Чимало українських дослідників, серед яких О. Баранов, Д. Белов, М. Белова, О. Головка, М. Гребенюк, І. Забара, І. Костенко, В. Фурашев, Є. Харитонов та інші наголошують на тому, що правові механізми регулювання інформаційних технологій в Україні поки що є недостатньо розвиненими, що обмежує можливості розвитку цифрового сектора.

Проте перспективні напрямки удосконалення адміністративно-правового регулювання інформаційних технологій в Україні потребують окремого дослідження, враховуючи останні євроінтеграційні здобутки України, нові глобалізаційні виклики, які постали перед українським суспільством, а також об'єктивну необхідність удосконалення чинного національного законодавства та юридичної практики у даній сфері суспільних відносин.

Постановка завдання. Метою наукової публікації є дослідження перспективних напрямів удосконалення адміністративно-правового регулювання інформаційних технологій в Україні

Методологія даної публікації ґрунтується на розумінні необхідності використання сучасних наукових підходів (цивілізаційного, синергетичного) та класичних методів наукового пізнання: законів та принципів діалектики, системного та структурно-функціонального методів, прийомів логіки, юридичної статистики, методології порівняльного законодавства, формально-юридичного методу та методу юридичного моделювання тощо.



Результати дослідження. Однією з основних проблем, що стоїть на заваді розвитку сфери використання інформаційних технологій є недостатня гармонізація національного законодавства з європейськими стандартами. Це перешкоджає входженню України до єдиного цифрового ринку Європейського Союзу та створює труднощі у міжнародній співпраці. Окрім цього, в українському законодавстві недостатньо врегульовані питання, що стосуються таких інноваційних технологій, як блокчейн, штучний інтелект та Інтернет речей. Відсутність відповідних правових норм створює правову невизначеність для учасників цифрового ринку. Крім того, недостатній рівень захисту інтелектуальної власності у сфері інформаційних технологій може гальмувати розвиток інноваційних рішень та стримувати залучення інвестицій в Україну.

Для подолання зазначених викликів необхідно здійснити комплексні заходи щодо вдосконалення нормативно-правового регулювання інформаційних технологій.

Першою нагальною задачею України, яка взяла непохитний курс на євроінтеграцію, є адаптація національного законодавства до стандартів Європейського Союзу (далі – ЄС).

Гармонізація українського законодавства з європейськими нормами є важливим кроком на шляху до повноцінної інтеграції України в глобальний цифровий простір. У сучасному світі, де інформація відіграє ключову роль, захист персональних даних стає не лише правовим питанням, а й важливим елементом довіри між державою, бізнесом та громадянами.

Однією з головних європейських ініціатив у цій сфері є Загальний регламент захисту даних (GDPR), який було ухвалено в ЄС у 2016 році та запроваджено у 2018 році. Цей документ став стандартом у сфері захисту персональних даних та встановив жорсткі вимоги до їх обробки, зберігання та передачі. Важливо, що дія цього регламенту поширюється не лише на країни ЄС, а й на будь-які компанії чи організації, які працюють з даними громадян Євросоюзу. Тобто, якщо українська ІТ-компанія, банк або інтернет-магазин обробляє дані європейських користувачів, вона автоматично повинна відповідати вимогам GDPR [6].

З огляду на курс на євроінтеграцію, Україна прагне гармонізувати своє законодавство з європейськими нормами, і GDPR тут відіграє важливу роль. Впровадження його положень допоможе вирішити одразу кілька ключових завдань.

По-перше, це дасть змогу підвищити рівень довіри до українських цифрових сервісів. В епоху цифрових технологій кожен із нас щодня залишає чималу кількість персональних даних в інтернеті — від банківської інформації до звичайних реєстрацій у соціальних мережах. Однак через кібератаки та витоки інформації, є ризик втрати персональних даних або використання їх третіми особами без дозволу суб'єкта цих даних. Впровадження стандартів GDPR гарантує прозорість та відповідальність у роботі з персональною інформацією, що автоматично підвищує рівень довіри з боку громадян.

По-друге, це суттєво зміцнить рівень захисту персональних даних громадян. GDPR передбачає чіткі правила щодо обробки персональної інформації. Наприклад, суб'єкт має право знати, які саме дані про неї збирають, як вони використовуються та з ким можуть бути поділені. Також кожен отримує право вимагати видалення своїх даних, якщо вони більше не потрібні компанії або були отримані незаконним шляхом. Запровадження таких правил в Україні допоможе більш усвідомлено керувати своєю цифровою приватністю.

По-третє, це значно підвищить конкурентоспроможність українського ІТ-сектору. Україна — один із найбільших постачальників ІТ-послуг у світі, і багато українських компаній працюють із європейськими замовниками. Однак для виходу на міжнародний ринок вони повинні відповідати жорстким вимогам щодо захисту даних. Якщо держава імплементує GDPR, це значно полегшить українським компаніям доступ до європейських клієнтів та інвесторів. Вони не тільки відповідатимуть міжнародним стандартам, але й отримають репутацію надійних партнерів, що позитивно вплине на розвиток цифрової економіки.

По-четверте, це дасть можливість долучитися до загальноєвропейських цифрових ініціатив. GDPR є лише одним із елементів глобальної цифрової стратегії Європейського Союзу. В ЄС активно розвивається концепція Єдиного цифрового ринку (Digital Single Market), яка спрямована на створення спільного простору для цифрових послуг, електронної



комерції та інновацій. Інтеграція України до цієї ініціативи відкриє нові можливості для бізнесу, спростить взаємодію між українськими та європейськими компаніями та зробить Україну повноцінним гравцем на цифровому ринку ЄС [7].

Проте на шляху імплементації GDPR в Україні стоїть чимало викликів, серед яких основним вбачається критична необхідність оновлення законодавства.

Наразі українське законодавство у сфері захисту персональних даних не відповідає стандартам GDPR. Тому першочерговим завданням є прийняття нових законодавчих актів, які б гармонізували національні норми із європейськими.

Окрім того, більшість українських компаній ще не до кінця розуміють вимоги GDPR або не готові до цих змін, оскільки дотримання регламенту вимагає значних фінансових та організаційних ресурсів зі сторони держави. Не зайвим буде й розроблення на державному рівні спеціальних освітніх програм та тренінгів для бізнесу, щоб допомогти їм адаптуватися до нових правил.

Варто зазначити, що GDPR передбачає жорстку відповідальність за порушення правил. Так, Регламентом передбачено двоступеневу систему штрафів, що залежить від рівня серйозності порушення. Менш значні порушення можуть каратися штрафами до 10 мільйонів євро або 2% від річного світового обороту компанії, залежно від того, яка сума є більшою (за недотримання вимог щодо повідомлення контролюючих органів про витік персональних даних; відсутність чіткої політики захисту даних у компанії; недостатній рівень безпеки під час обробки персональних даних). Серйозні порушення караються штрафами до 20 мільйонів євро або 4% від глобального річного доходу компанії (за незаконний збір, обробку чи передачу персональних даних без згоди користувача; недотримання основних принципів GDPR, таких як прозорість обробки даних або право на забуття; використання персональних даних для цілей, не передбачених законодавством [4].

Яскравим прикладом реального застосування штрафних санкцій є випадки з великими технологічними компаніями. Так, Amazon у 2021 році був оштрафований на 746 мільйонів євро за порушення правил обробки персональних даних. Google у 2019 році отримав штраф у 50 мільйонів євро за недостатню прозорість у використанні персональних даних користувачів. Meta (Facebook) у 2023 була оштрафована на 1,2 мільярда євро за незаконну передачу даних користувачів до США.

Крім того, однією з ключових проблем є те, що в Україні немає незалежного органу, який би відповідав за нагляд за дотриманням норм захисту персональних даних на рівні, аналогічному до європейських моделей. У країнах ЄС такі органи є: Data Protection Commission (DPC) в Ірландії, CNIL (Commission Nationale de l'Informatique et des Libertés) у Франції, ICO (Information Commissioner's Office) у Великій Британії [3].

Ці установи здійснюють моніторинг дотримання GDPR, розглядають скарги громадян, проводять розслідування та накладають штрафи. В Україні цю роль частково виконує Уповноважений Верховної Ради України з прав людини, однак цей орган не має таких повноважень та ресурсів, як його європейські аналоги.

Отже, запровадження норм GDPR в Україні — це не лише питання законодавства, а й свідомий стратегічний крок до зміцнення цифрової економіки, захисту персональних даних громадян та інтеграції у європейський цифровий простір. Впровадження європейських стандартів підвищить рівень довіри до українських цифрових сервісів, сприятиме розвитку бізнесу та відкриє нові можливості для міжнародної співпраці. Україна вже робить перші кроки у цьому напрямку, і гармонізація законодавства з європейськими нормами стане вагомим етапом на шляху до цифрового майбутнього країни.

Іншим перспективним напрямом України є правове регулювання інноваційних технологій, зокрема, розробки законодавчих механізмів для регулювання блокчейн-технологій, штучного інтелекту та інтернету речей. Створення чітких правових засад у цих сферах забезпечить прозорість роботи цифрового ринку, сприятиме інвестиціям та розвитку стартап-екосистеми.

Україна вже намагалась здійснити певні кроки у цьому напрямку, зокрема, ухваливши Закон України «Про віртуальні активи». Водночас цей нормативний акт не набув чинності



через необхідність додаткових змін до Податкового кодексу, що визначатимуть механізми оподаткування операцій з цифровими активами. Відсутність врегульованого підходу до оподаткування віртуальних активів стримує розвиток крипторинку в країні [5].

Історія Закону України «Про віртуальні активи» наглядно показала, як складно поєднати інновації, економічну стабільність та міжнародні зобов'язання. Однак є сподівання, що у майбутньому, з урахуванням досвіду інших країн та власних уроків, Україна має шанс створити ефективне правове середовище для крипторинку, яке сприятиме його розвитку та водночас захищатиме інтереси держави і громадян.

Актуальним й водночас перспективним напрямом України є правове регулювання Штучного інтелекту.

Штучний інтелект (далі - ШІ) є однією з найперспективніших технологій сучасності, яка може суттєво вплинути на економіку, державне управління, освіту, медицину та багато інших сфер. Україна, яка активно розвиває цифрову економіку, має всі передумови для того, щоб стати лідером у розробці та впровадженні ШІ-рішень. Однак для цього необхідно створити сприятливі умови як на рівні державної підтримки, так і у правовому полі.

Штучний інтелект вже давно перестав бути просто концепцією з наукової фантастики. Він став частиною повсякденного життя людини: від голосових помічників у смартфонах до систем прогнозування у фінансовій сфері та навіть самокерованих автомобілів. Однак, разом із цими можливостями постає низка складних юридичних та етичних питань, на які суспільству ще належить знайти відповіді.

На сьогодні в більшості країн немає єдиного підходу до визначення відповідальності за дії автономних систем. У деяких випадках, як-от з самокерованими автомобілями, обов'язок покладається на виробника, якщо несправність сталася через технічну помилку. Але якщо рішення ухвалював алгоритм, створений на основі машинного навчання, визначити винного стає набагато складніше.

Так, Є. Харитонов зазначає, що при сприятливих умовах розвитку людства проблема визнання штучного інтелекту суб'єктом права вже в недалекому майбутньому може постати на повний зріст. Тому маємо бути готовими до такого перебігу подій. У кожному разі вже зараз має бути встановлена принципова можливість і методологічне підґрунтя «суб'єктивізації» Штучного інтелекту, тобто визнання за ним властивостей суб'єкта (квазі-суб'єкта) правовідносин. [1].

Один із можливих підходів – принцип «людиноцентричного» штучного інтелекту, який передбачає, що остаточні рішення, які мають значний вплив на людину (наприклад, у медицині, фінансах чи правосудді), повинні ухвалюватися не лише алгоритмом, а й людиною. Це дозволить уникнути ситуацій, коли ШІ ухвалює рішення, які можуть негативно вплинути на права громадян, без можливості людського втручання.

На сьогодні в Україні немає спеціального законодавства, яке б визначало правила використання ШІ, відповідальність за його дії та механізми захисту персональних даних.

Водночас у Європейському Союзі 13 березня 2024 року було ухвалено Закон про штучний інтелект (Artificial Intelligence Act), який передбачає обов'язкову прозорість для високо-ризикових систем ШІ. Це означає, що розробники повинні пояснювати, як працює алгоритм, які дані він використовує та які можуть бути потенційні ризики його застосування. [8].

Україна, прагнучи інтегруватися до ЄС, повинна розробити національну стратегію регулювання ШІ, що має охоплювати такі важливі аспекти як: 1) визначення відповідальності за дії ШІ (якщо штучний інтелект ухвалює рішення, які призводять до негативних наслідків, має бути чітко визначено, хто несе відповідальність: розробник програмного забезпечення, власник або оператор системи або ж держава (якщо ШІ використовується у державному управлінні); 2) захист персональних даних (ШІ-системи працюють на основі великих масивів даних, що включають персональну інформацію користувачів, тому важливо гарантувати, що дані збиратимуться та оброблятимуться відповідно до міжнародних стандартів (наприклад, норм GDPR (General Data Protection Regulation), які вже діють в ЄС); 3) запровадження етичних стандартів (для того щоб уникнути дискримінації та упередженості у рішеннях ШІ,



потрібно розробити етичні стандарти для його використання, що особливо важливо у сферах фінансів, правосуддя та медицини. Наприклад, алгоритми не повинні приймати рішення, які можуть порушувати права людини або бути упередженими за статтю, расою чи соціальним статусом).

Деякі країни, такі як Канада, США та Китай, уже розробили свої національні стратегії розвитку Штучного інтелекту. Україна також має рухатися в цьому напрямку та ухвалити Національну стратегію розвитку штучного інтелекту, яка визначатиме ключові пріоритети та напрями підтримки цієї технології.

Штучний інтелект відкриває перед Україною широкі можливості для економічного та технологічного зростання. Однак для повноцінного використання цього потенціалу необхідно створити ефективну систему правового регулювання, яка гарантуватиме прозорість, безпеку та відповідальність за її використання.

Окремої уваги в розрізі перспектив удосконалення нормативно-правового регулювання інформаційних технологій України заслуговує питання правового регулювання Інтернету речей.

Простими словами Інтернет речей (Internet of Things, IoT) це мережа пристроїв, що з'єднані між собою через Інтернет для збору, передачі та аналізу даних. IoT є частиною повсякденного життя людини. Впровадження IoT дозволяє оптимізувати процеси, економити ресурси і створювати нові сервіси. Смартфони, смарт-годинники, «розумні» камери спостереження, «розумні» будинки, системи управління енергоспоживанням і навіть автономні транспортні засоби — усе це приклади IoT, які поступово стають звичними. Однак разом із розвитком цих технологій виникає потреба у створенні відповідного нормативно-правового регулювання. Україна, прагнучи інтегруватися в європейський цифровий простір, також повинна звернути увагу на цей виклик.

В той же час, необхідно визнати, що існують певні бар'єри та ризики на шляху розвитку технологій Інтернету речей в Україні.

Так, О. Баранов зазначає, що до основних проблем на шляху розвитку IoT слід віднести відсутність державної стратегії та лідерів змін, недостатнє розуміння цінностей IP політичним істеблшментом країни, керівниками галузей та бізнес-структур. Крім того, існує ще певна низка бар'єрів та ризиків: політичні, техніко-технологічні, правового регулювання, освітнянські та мотиваційні, фінансово-економічні, правового регулювання, безпекові, конфіденційності, сумісності, стандартизації. Кожен з перелічених видів бар'єрів потребує ретельного дослідження для формування програми заходів щодо їх подолання [2].

На сьогодні в Україні відсутній єдиний нормативно-правовий акт, який регулює сферу IoT. Хоча окремі аспекти цієї технології регулюються законами про електронні комунікації, кібербезпеку та захист персональних даних, комплексного підходу немає. Це створює прогалини, які можуть бути використані недобросовісними компаніями.

Так, М. Белова зазначає, що законодавство України повинно вимагати від виробників IoT-пристроїв дотримання базових стандартів безпеки, таких як шифрування даних та регулярне оновлення програмного забезпечення. А сертифікація IoT-пристроїв гарантуватиме їхню безпеку та відповідність стандартам. Це все підвищить довіру користувачів до нових технологій [3].

Таким чином, Інтернет речей відкриває перед Україною величезні можливості, але водночас ставить серйозні виклики. Без належного регулювання впровадження IoT може стати джерелом ризиків для приватності, безпеки та економіки. Проте, якщо створити ефективне нормативно-правове середовище, Україна зможе стати лідером у впровадженні IoT у регіоні, залучаючи інвестиції, розвиваючи інновації та підвищуючи якість життя своїх громадян.

З огляду на необхідність створення, удосконалення та узгодження між собою норм у сфері інформаційних технологій перспективним напрямом удосконалення адміністративно-правового регулювання інформаційних технологій в Україні вбачається уніфікація та кодифікація національного законодавства, що регулює сферу інформаційних технологій.



Ще одним важливим напрямком удосконалення адміністративно-правового регулювання використання інформаційних технологій в Україні може стати уніфікація та кодифікація законодавства у цій сфері.

Україна, прагнучи інтегруватися до глобального цифрового простору, активно розвиває нормативно-правову базу у цій сфері. Однак, наявні законодавчі акти часто розпорошені, що ускладнює їх застосування та створює правову невизначеність. У цьому контексті постає питання про необхідність створення Цифрового кодексу України як єдиного кодифікованого акту, який би систематизував та унормував правовідносини у цифровій сфері.

Фрагментарність чинного законодавства призводить до прогалин та колізій, що можуть стримувати інновації та створювати ризики для учасників цифрового ринку. Цифровий кодекс дозволить об'єднати розрізнені нормативні акти, забезпечивши цілісність та узгодженість правового регулювання. Такий підхід сприятиме підвищенню правової визначеності, прозорості та передбачуваності у сфері інформаційних технологій.

Деякі країни вже зробили кроки до кодифікації цифрового законодавства. Наприклад, Європейський Союз прийняв Європейський кодекс електронних комунікацій, який об'єднує основні положення щодо електронних комунікацій та встановлює єдині правила для країн-членів [9].

Україна, орієнтуючись на європейський досвід, може розробити власний Цифровий кодекс, враховуючи національні особливості та потреби.

Варто зазначити, що запровадження Цифрового кодексу України матиме низку переваг, серед яких: 1) систематизація законодавства (об'єднання розрізнених нормативних актів у єдиний документ спростить їх застосування та підвищить ефективність правового регулювання); 2) гармонізація з міжнародними стандартами (адаптація європейського досвіду сприятиме інтеграції України до глобального цифрового простору та підвищенню конкурентоспроможності на міжнародному ринку); 3) захист прав громадян та бізнесу (чітке визначення цифрових прав та обов'язків забезпечить захист інтересів усіх учасників цифрових відносин); 4) стимулювання інновацій (створення сприятливого правового середовища сприятиме розвитку новітніх технологій та залученню інвестицій у ІТ-сектор).

З огляду на вищевикладене, створення Цифрового кодексу України є необхідним кроком для забезпечення ефективного та сучасного правового регулювання у сфері інформаційних технологій. Такий кодифікований акт стане важливим етапом на шляху до побудови розвиненого цифрового суспільства в Україні.

Таким чином, перспективи нормативно-правового забезпечення інформаційних технологій в Україні базуються на необхідності комплексної модернізації законодавства, його гармонізації з міжнародними стандартами, уніфікації та кодифікації законодавства, а також, запровадженні сучасних технологічних рішень та розвитку правової культури у цифровій сфері. За таких умов Україна матиме шанс стати повноцінним учасником глобального цифрового суспільства.

Висновки. Проведене дослідження дозволяє визначити перспективні напрями удосконалення адміністративно-правового регулювання інформаційних технологій в Україні шляхом внесення відповідних змін до чинного національного законодавства та приведення його у відповідність до норм та принципів права ЄС.

Зокрема, об'єктивною є потреба у подальшій гармонізації українського законодавства з європейськими нормами, що є необхідною передумовою на шляху до повноцінної інтеграції України в глобальний цифровий простір.

Перспективні напрями адміністративно-правового регулювання інформаційних технологій в Україні, окрім адаптації національного законодавства до стандартів Європейського Союзу, включають створення ефективних механізмів регулювання інноваційних технологій та захист персональних даних. Також, об'єктивною є потреба в уніфікації та кодифікації законодавства у сфері інформаційних технологій. Все це разом сприятиме розвитку цифрової економіки та інтеграції України у світовий інформаційний простір.

Перспектива подальшого дослідження даної теми обумовлена необхідністю



формулювання конкретних пропозицій щодо внесення змін до чинного національного законодавства у сфері інформаційних технологій.

Список використаних джерел:

1. Харитонов Є. О., Харитонova О. І. Правовідносини та штучний інтелект: «суб'єктивізація» об'єкту. Збірник наукових праць. Київ, 2019. С. 23–30. URL: https://ippi.org.ua/sites/default/files/maket_ot_20.11.19_1.pdf.
2. Баранов О. А. Інтернет речей і право: погляд у майбутнє. Інтернет речей: проблеми правового регулювання та впровадження: Збірник наукових праць. Київ, 2019. С. 7–12. URL: https://ippi.org.ua/sites/default/files/maket_ot_20.11.19_1.pdf.
3. Белова М. В., Белов Д. М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 79, ч. 2. С. 17-22. DOI: <https://doi.org/10.24144/2307-3322.2023.79.2.2>.
4. General Data Protection Regulation (GDPR): що це означає для України? *Закон і Бізнес*: Юридична газета. 2018. URL: https://zib.com.ua/ua/133137-general_data_protection_regulation.html.
5. Про віртуальні активи: Закон України від 17 лютого 2022 р. № 2074-IX. Дата оновлення: 16.03.2022. URL: <https://zakon.rada.gov.ua/laws/show/2074-IX>.
6. General Data Protection Regulation (GDPR). Регламент ЄС 2016/679. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>.
7. Європейська комісія. Digital Single Market Strategy. URL: <https://digital-strategy.ec.europa.eu/en>.
8. Artificial Intelligence Act. Європейський Союз. Офіційний портал законодавства ЄС, 2024. URL: <https://digital-strategy.ec.europa.eu/en/library/artificial-intelligence-act>.
9. Європейський кодекс електронних комунікацій (European Electronic Communications Code). Європейський Союз, 2024. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972>.

