

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНСТИТУЦІЙНОЇ ПРИВАБЛИВОСТІ ІТ-СЕКТОРУ УКРАЇНИ В КОНТЕКСТІ ГЛОБАЛЬНОГО МАРКЕТИНГУ ЦИФРОВИХ ПОСЛУГ

ПОПКО Олена Володимирівна

*докторка економічних наук, професорка,
професорка кафедри маркетингу*

Національного університету водного господарства та природокористування

ORCID ID: <https://orcid.org/0000-0003-3356-6070>

ТИВОНЧУК Павло Вікторович

здобувач ступеня доктора філософії

Національного університету водного господарства та природокористування

ORCID ID: <https://orcid.org/0009-0006-6378-7228>

Анотація. Метою статті є системний аналіз нормативно-правового регулювання ІТ-галузі України та порівняльне дослідження зарубіжного досвіду для обґрунтування напрямів удосконалення законодавства. Дослідження охоплює три структурні виміри: спеціальний режим оподаткування та зайнятості Дія City, захист персональних даних і кібербезпеку, охорону інтелектуальної власності в цифровому середовищі. Установлено, що чинне регулювання утворює фрагментарну систему з понад двадцяти спеціальних законів без єдиного кодифікованого акта. Ефективність режиму Дія City підтверджено вимірюваними показниками: кількість резидентів зросла з 72 у I кварталі 2022 р. до 1 287 наприкінці 2024 р., сукупний персонал перевищив 84 тис. фахівців, середня заробітна плата досягла 2 510 євро на місяць, частка гіг-контрактів становить 72 %. Виявлено вразливості режиму: псевдогігізацію, звуження захисту від перевірок в умовах воєнного стану, непоширення механізму бронювання на гіг-спеціалістів. Окремо розглянуто прогалини регулювання оборонних технологій (MilTech) та експортного контролю програмного забезпечення подвійного призначення. Аргументовано потребу законодавчого визнання смарт-контрактів і гармонізації регулювання віртуальних активів із Регламентом МіСА. Порівняння з регуляторними моделями ЄС (GDPR, DSA, DMA, AI Act), Естонії, Сінгапуру та Ізраїлю засвідчило відставання України за трьома напрямками: відсутність законодавства про штучний інтелект, неврегульованість транскордонної передачі даних, нерозвиненість обов'язкових кіберстандартів для приватного сектору (25-те місце в рейтингу ITU GCI 2024). Сформульовано матрицю з восьми законодавчих реформ із визначенням пріоритетів і строків. Обґрунтовано, що правове реформування є інструментом маркетингового просування українських цифрових послуг на глобальному ринку.

Ключові слова: ІТ-галузь; Дія City; регулювання цифрової економіки; захист персональних даних; кібербезпека; GDPR; інтелектуальна власність; гіг-контракти; регулювання штучного інтелекту.

Постановка проблеми. Питання правового забезпечення діяльності ІТ-компаній в Україні набуло якісно нового виміру після лютого 2022 року — в умовах повномасштабного збройного вторгнення та прискореної цифрової трансформації держави. За даними Міністерства цифрової трансформації, у 2023 році ІТ-галузь забезпечила 4,7% ВВП країни, а надходження від експорту ІТ-послуг становили 7,3 млрд доларів США [1, С. 12].

Ці показники засвідчують, що ІТ-сектор перетворився на один із системоутворюючих елементів національної економіки, правове регулювання якого безпосередньо впливає на конкурентоздатність держави на глобальному ринку. Правова архітектура регулювання ІТ-сектору в Україні формувалася поетапно: від перших законодавчих актів у сфері інформатизації початку 2000-х років до запровадження режиму Дія City у 2021 році. Упродовж усього цього шляху законодавець стикався з фундаментальним викликом — необхідністю забезпечити правову визначеність у галузі, що технологічно розвивається швидше, ніж встигає реагувати нормативна система. В.О. Апалькова та І.М. Грищенко встановили, що розрив між технологічними реаліями та правовим регулюванням у цифровій сфері становить від трьох до семи років [4, С. 34]. Скажемо відверто: жоден із чинних законів не охоплює регулювання ні штучного інтелекту, ні Web3-технологій, ні децентралізованих фінансів — трьох технологічних трендів, що формуватимуть ІТ-риннок наступного десятиліття.

Окремої уваги потребує стан імплементації Закону України «Про віртуальні активи» від 17 лютого 2022 року № 2074-IX. Попри набуття чинності, закон залишається фактично недієвим через відсутність підзаконної нормативної бази та несформованість регуляторного органу — Національної комісії з цінних паперів та фондового ринку у відповідній функції. Це створює парадоксальну ситуацію: ринок криптоактивів в Україні юридично легалізовано, однак механізми його практичного регулювання відсутні.

Водночас Євросоюз із 30 грудня 2024 року розпочав повноцінне застосування Регламенту MiCA (Markets in Crypto-Assets, Reg. EU 2023/1114), який встановлює єдині правила для емітентів криптоактивів і постачальників послуг у сфері криптоактивів на всьому просторі ЄС. Для України, що перебуває на шляху до євроінтеграції, гармонізація вітчизняного законодавства про віртуальні активи з MiCA є не лише доцільною, але й неминучою умовою доступу українських Web3-компаній до ринків ЄС. Зокрема, це стосується вимог до ліцензування постачальників послуг із криптоактивів (CASP), стандартів розкриття інформації в white paper, а також механізмів захисту споживачів при операціях із стейблкоїнами.

Гармонізація з MiCA охоплює переважно обіг криптоактивів, проте поза увагою законодавця залишається фундаментальніше питання — юридична сила смарт-контрактів як самостійної форми правочину. Чинний Цивільний кодекс України оперує класичною конструкцією правочину, що передбачає волевиявлення сторін у письмовій або електронній формі, тоді як смарт-контракт є самовиконуваним програмним кодом, який автоматично реалізує домовленість при настанні заздалегідь визначених умов без подальшого втручання сторін. Це породжує низку невирішених питань: чи визнається алгоритмічний код формою волевиявлення; який момент вважати укладенням такого договору; як співвідносяться автоматичне виконання та інститути недійсності правочину, помилки й істотної зміни обставин; нарешті, хто несе відповідальність за збій у коді, що призвів до майнової шкоди. У зарубіжній практиці окреслилися два підходи — визнання смарт-контракту самостійним видом

договору або його кваліфікація як технічного способу виконання звичайного зобов'язання. Для усунення правової невизначеності доцільно доповнити Цивільний кодекс України нормами, що прямо визнають за алгоритмічним кодом здатність виражати волю сторін правочину та встановлюють співвідношення між автоматичним виконанням смарт-контракту й загальними положеннями зобов'язального права. Без такого регулювання Web3-сегмент української економіки розвиватиметься в умовах перманентного ризику невизнання судами укладених у такий спосіб домовленостей.

Ситуацію ускладнює відсутність єдиного кодифікованого акту — на відміну від ЄС, де Digital Services Act 2022 року та Digital Markets Act 2022 року формують цілісну регуляторну надбудову над галузевим законодавством держав-членів. Натомість в Україні нормативне поле складається з понад двадцяти спеціальних законів та численних підзаконних актів, що у своїй сукупності утворюють фрагментарну систему з очевидними прогалинами. Н.М. Краус та К.М. Краус кваліфікують подібну архітектуру як «спонтанний регуляторний пуризм» — законодавче реагування на вже сформовані технологічні практики замість випереджального нормотворення [3, С. 81].

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання цифрової економіки перебуває у фокусі активного наукового дискурсу. Концептуальні засади цифрової трансформації суспільства у правовому вимірі розроблено у монографії О. С. Вишневського [6], а правові аспекти цифрової індустріалізації України досліджено В. І. Ляшенком та О. А. Вишневською [7]. Еволюцію парадигм регулювання цифрової економіки — від «інформаційної» до «екосистемної» — простежено у працях Г. М. Пилипенко [9]. Режим Дія City як інноваційну правову платформу проаналізовано Н. М. Краус та К. М. Краус [3], які звернули увагу на реактивний характер вітчизняного нормотворення. Правову природу гіг-контрактів та практику їх застосування досліджено Л. П. Гаращенко [10], порівняльну характеристику правових форм залучення ІТ-фахівців — О. В. Чорною [11], а ризики псевдогігізації — А. Г. Тополем [14]. Колізії захисту бізнесу від перевірок в умовах воєнного стану висвітлено О. В. Марченко [12]. Проблему співіснування вітчизняного законодавства про персональні дані та GDPR («подвійне регуляторне навантаження») розкрито О. В. Карпенком [15], а регуляторний потенціал незалежного наглядового органу — В. М. Кравченком [21]. Питання термінологічної визначеності в ІТ-законодавстві порушено В. В. Харченком та О. В. Карпенком [5], розрив між технологічними реаліями та правовим регулюванням кількісно оцінено В. В. Апальковою та І. М. Грищенком [4]. Зарубіжний досвід представлено дослідженнями естонської моделі е-урядування Л. Д. Тімченко та Н. О. Рибачок [20] і концептуальними працями L. Floridi та J. Cowsls щодо принципів регулювання штучного інтелекту [8].

Водночас, попри вагомий науковий доробок, комплексного дослідження нормативно-правового забезпечення ІТ-галузі, яке поєднувало б аналіз ефективності режиму Дія City в умовах воєнного стану, порівняння з регуляторними моделями провідних цифрових юрисдикцій та розгляд правової реформи як інструменту глобального маркетингу цифрових послуг, у вітчизняній науці досі не здійснено. Це й зумовлює актуальність цієї статті.

Мета статті — системний аналіз нормативно-правової бази регулювання ІТ-галузі в Україні та порівняльне дослідження міжнародного досвіду задля формулювання обґрунтованих практичних рекомендацій щодо вдосконалення вітчизняного законодавства. Для досягнення мети вирішено три дослідницьких

завдання: по-перше, систематизація та класифікація чинних нормативно-правових актів у сфері ІТ; по-друге, оцінювання ефективності режиму Дія City як правового інструменту в умовах воєнного стану; по-третє, порівняльний аналіз регуляторних моделей ЄС, Естонії, Сінгапуру та Ізраїлю.

Наукова новизна дослідження. Наукова новизна одержаних результатів полягає в такому: уперше здійснено комплексний порівняльний аналіз нормативно-правового забезпечення ІТ-галузі України з регуляторними моделями ЄС, Естонії, Сінгапуру та Ізраїлю з урахуванням трансформацій періоду воєнного стану (2022–2024 рр.) та обґрунтовано розгляд правової реформи як інструменту маркетингового просування українських цифрових послуг на глобальному ринку; удосконалено структурну класифікацію нормативно-правового регулювання ІТ-галузі за чотирма вимірами (суб'єктним, об'єктним, процесуальним та юрисдикційним) з оцінюванням рівня розробленості кожного з них; набули подальшого розвитку положення щодо системних вразливостей режиму Дія City (псевдогігізація, непоширення механізму бронювання на гіг-спеціалістів, звуження захисту від перевірок) та науково-практичні рекомендації щодо гармонізації вітчизняного законодавства з *acquis* ЄС, формалізовані у вигляді матриці восьми законодавчих реформ із визначенням пріоритетів і строків реалізації.

Виклад основних результатів дослідження. Дослідження виходить із розуміння, що нормативно-правове забезпечення виступає фундаментом маркетингової стратегії просування українських цифрових послуг на глобальних ринках: правові реформи формують довіру іноземних замовників, знижують юрисдикційні ризики та створюють цінову привабливість галузі. Відтак удосконалення регуляторного середовища розглядається не як самоціль, а як інструмент підвищення інституційної привабливості України у глобальній конкуренції за замовників, інвесторів і таланти

Розуміння природи нормативно-правового регулювання ІТ-галузі передбачає насамперед визначення меж самого поняття «ІТ-галузь» у правовому вимірі. На відміну від традиційних секторів економіки — промисловості, сільського господарства, фінансів — ІТ-сфера не має усталеної правової дефініції ні в українському, ні в міжнародному законодавстві. Законодавець у різних актах послуговується поняттями «інформаційні технології», «програмне забезпечення», «цифрові послуги», «електронна комерція» та «інформаційно-комунікаційні технології» (ІКТ), що несуть неоднакове смислове навантаження і породжують труднощі при розмежуванні сфер правового регулювання [5, С. 23]. Ця термінологічна розпорошеність — не лише філологічна проблема: від дефініції залежить, які саме компанії підпадають під той чи інший правовий режим.

Узагальнивши підходи О.С. Вишневського [6, С. 44], В.І. Ляшенка [7, С. 112] та зарубіжного дослідника L. Floridi [8, С. 78], регулювання ІТ-галузі правомірно структурувати за чотирма вимірами: суб'єктним (правовий статус учасників ІТ-ринку), об'єктним (регулювання програмного забезпечення, баз даних, алгоритмів, персональних даних, цифрових активів), процесуальним (порядок здійснення ІТ-діяльності: ліцензування, захист даних, аудит) та юрисдикційним (питання застосовного права у транскордонних відносинах). Жоден із зазначених вимірів у чинному українському законодавстві не отримав вичерпного нормативного оформлення.

Структурна класифікація нормативно-правового регулювання ІТ-галузі України

Вимір регулювання	Основні нормативні акти	Розробленість (1–5)	Системні прогалини
Суб'єктний	ЗУ «Про стимулювання розвитку цифрової економіки», ЗУ «Про зайнятість населення»	4	Правовий статус DAO-учасників, ІІІ-агентів
Об'єктний	ЗУ «Про авторське право», ЗУ «Про захист персональних даних»	3	Алгоритмічні системи, NFT, цифрові активи
Процесуальний	ЗУ «Про захист інформації в ІКС», ЗУ «Про кібербезпеку»	3	Відповідальність за витоки даних, аудит ІІІ
Юрисдикційний	Будапештська конвенція, GDPR (de facto)	2	Транскордонні дані, SaaS-договори, хмарна юрисдикція

Джерело: складено авторами на основі аналізу законодавства України.

Наведена структура засвідчує глибоку асиметрію регуляторного розвитку: якщо суб'єктний вимір отримав відносно повне оформлення завдяки Дія City, то юрисдикційний залишається фактично поза правовим полем. Між тим, саме юрисдикційні питання стають дедалі гострішими в міру того, як українські ІТ-компанії розширюють присутність на ринках ЄС, США та Азіатсько-Тихоокеанського регіону.

В умовах відсутності спеціального законодавства про штучний інтелект Міністерство цифрової трансформації України обрало стратегію «м'якого» регулювання (soft law), що передбачає розробку добровільних галузевих стандартів, рекомендаційних кодексів поведінки та механізмів саморегулювання ринку. Подібний підхід узгоджується з міжнародним досвідом: Сінгапур до ухвалення обов'язкових норм тривалий час застосовував рекомендаційний Model AI Governance Framework (2019, ред. 2020), а Велика Британія поки утримується від єдиного обов'язкового закону про ІІІ на користь галузевого саморегулювання.

Разом із тим українські компанії вже зараз мають практичну потребу готуватися до вимог EU AI Act, що набуде повної чинності у серпні 2026 року. Передусім це стосується систем «високого ризику» відповідно до Додатку ІІІ Регламенту — зокрема, AI-систем у сферах зайнятості, освіти, біометричної ідентифікації та управління критичною інфраструктурою. Для таких систем EU AI Act вимагає: ведення технічної документації та журналів аудиту, оцінки відповідності до введення в експлуатацію, прозорого інформування кінцевих користувачів, а також призначення уповноваженої особи з питань відповідності (compliance officer). Українські ІТ-компанії, що постачають подібні системи на ринок ЄС або використовують їх у власній діяльності, підпадатимуть під екстратериторіальну дію регламенту незалежно від наявності чи відсутності вітчизняного аналога.

Юрисдикційний вимір регулювання потребує окремого аналізу з огляду на масштаб практичної проблеми. Абсолютна більшість великих українських ІТ-компаній використовує хмарні сервіси іноземних провайдерів — Amazon Web

Services (AWS), Microsoft Azure та Google Cloud Platform, — чиї сервери фізично розташовані поза межами України. Це породжує фундаментальну колізію: Закон України «Про захист інформації в інформаційно-комунікаційних системах» (1994, ред. 2005) та підзаконні акти ДССЗІ містять вимоги щодо зберігання певних категорій інформації на серверах в Україні, тоді як комерційна логіка та вимоги клієнтів із ЄС диктують використання євро-регіональних дата-центрів.

Окремою прогалиною залишається правове регулювання SaaS-договорів (Software as a Service). На відміну від традиційних ліцензійних угод на програмне забезпечення, SaaS-відносини характеризуються: відсутністю передачі примірника програми, безперервним характером надання послуги, обробкою даних клієнта на стороні постачальника та складністю визначення місця виконання зобов'язання для цілей застосовного права. Жоден чинний нормативний акт України прямо не регулює ані SaaS-договір як окремий вид, ані питання «хмарної юрисдикції» — тобто визначення права, застосовного до договірних і позадоговірних відносин, що виникають при транскордонній обробці даних у хмарному середовищі. Запровадження механізму стандартних договірних застережень (Standard Contractual Clauses), рекомендованого в реформі № 4 матриці (таблиця 11), має вирішувати саме цю прогалину шляхом уніфікації договірних підстав транскордонної передачі даних за зразком Рішення Єврокомісії 2021/914.

Становлення нормативно-правового забезпечення ІТ-сфери в Україні охоплює чотири виразних етапи, кожен із яких зумовлений поєднанням технологічних, економічних та політичних чинників. Г.М. Пилипенко класифікує ці етапи за критерієм домінантної регуляторної парадигми: від «інформаційного» через «телекомунікаційний» та «цифрово-комерційний» до сучасного «екосистемного» підходу [9, С. 56].

Перший етап (1994–2010) визначався прийняттям базових законів у сфері інформатизації та інформаційного захисту. Закон «Про Національну програму інформатизації» 1998 року та Закон «Про захист інформації в інформаційно-комунікаційних системах» 1994 року заклали основу технічного регулювання, однак орієнтувалися передовсім на потреби державного сектору, залишаючи ринок ІТ-послуг практично поза правовим полем. Другий етап (2010–2017) позначився прийняттям Закону «Про захист персональних даних» (2010), ратифікацією Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108), а також запровадженням базового законодавства про електронну комерцію (2015). Третій етап (2017–2021) охоплює Закон «Про основні засади забезпечення кібербезпеки України» (2017), затвердження Стратегії кібербезпеки України та підготовку до прийняття нової редакції Закону «Про авторське право і суміжні права» 2022 року. У цей період Україна активно імплементувала положення Угоди про асоціацію з ЄС, що зумовило часткову гармонізацію у сферах захисту даних та інтелектуальної власності [10, С. 67]. Четвертий, нинішній етап (2021 — по теперішній час) відкрився прийняттям Закону «Про стимулювання розвитку цифрової економіки в Україні» від 15 липня 2021 року (№ 1667-IX), що запровадив режим Дія City — принципово новий правовий конструкт у вітчизняному законодавстві.

Таблиця 2

**Хронологія розвитку нормативно-правової бази ІТ-сфери України
(1994–2024 рр.)**

Рік	Нормативний акт	Регуляторна новація	Контекст прийняття
1994	ЗУ «Про захист інформації в ІКС»	Технічний захист даних у держсекторі	Становлення незалежності
1998	ЗУ «Про Національну програму інформатизації»	Державна стратегія ІКТ-розвитку	Рання цифровізація
2003	ЗУ «Про електронний цифровий підпис»	Легалізація електронного документообігу	Адаптація до вимог WTO
2010	ЗУ «Про захист персональних даних»	Перший закон про персональні дані	Євроінтеграційний курс
2015	ЗУ «Про електронну комерцію»	Регулювання онлайн-торгівлі	Угода про асоціацію з ЄС
2017	ЗУ «Про основні засади кібербезпеки»	Стратегічна кібербезпека держави	Гібридна агресія РФ
2021	ЗУ «Про стимулювання розвитку цифрової економіки»	Режим Дія City, гіг-контракти	Конкуренція за ІТ-таланти
2022	ЗУ «Про авторське право» (нова ред.)	Цифрова інтелектуальна власність	Повномасштабна агресія РФ
2024	Зміни до ЗУ «Про стимулювання...»	Розширення Дія City в умовах воєнного стану	Збереження ІТ-галузі

Джерело: складено авторами за матеріалами Верховної Ради України [13].

Таблиця 3

Основні показники ІТ-сектору України (2019–2024 рр.)

Показник	2019	2020	2021	2022	2023	2024
Обсяг ІТ-експорту, млрд USD	4,2	5,0	6,8	6,3	7,3	7,8*
Частка у ВВП, %	3,5	4,0	4,9	4,2	4,7	5,1*
Кількість ІТ-фахівців, тис. осіб	185	200	228	195	240	265*
Середня зарплата в ІТ, USD/міс.	1 850	2 100	2 450	2 200	2 380	2 510*
Кількість компаній-резидентів Дія City	—	—	72	311	863	1 287
ІТ-інвестиції (венчурний капітал), млн USD	380	290	470	180	320	420*

*Джерело: складено авторами за даними Мінцифри, IT Ukraine Association [1; 2]. * — попередні дані.*

Зіставлення даних таблиці 3 виявляє знакову закономірність: незважаючи на повномасштабне вторгнення 2022 року, що призвело до тимчасового скорочення

обсягів ІТ-експорту на 7,4% та відтоку близько 35 000 фахівців за кордон, галузь відновила зростання вже у 2023 році — і перевершила довоєнні показники. Це свідчить про структурну стійкість сектору, що багато в чому забезпечена саме правовою архітектурою Дія City.

Режим Дія City, запроваджений Законом України № 1667-ІХ, являє собою спеціальний правовий режим, що встановлює особливі умови для резидентів у сферах оподаткування, трудового права та захисту від надмірного державного контролю. За правовою природою Дія City поєднує елементи особливої економічної зони (без географічної прив'язки), спеціального податкового режиму та саморегулювальної системи для ІТ-компаній. Дослідниця Л.П. Гаращенко зазначає, що концептуально Дія City є найближчим аналогом британського Innovate UK та сінгапурського Tech@SG, однак вирізняється більш розвиненим механізмом захисту від перевірок [10, С. 67].

Для отримання статусу резидента компанія зобов'язана відповідати сукупності кваліфікаційних критеріїв: не менше 90% виручки від ІТ-діяльності; середня заробітна плата спеціалістів — щонайменше 1 200 євро на місяць; мінімальна кількість кваліфікованих ІТ-фахівців у штаті або за гіг-контрактами — не менше дев'яти осіб. Принципово, що закон унормував тривимірну модель взаємодії компанії зі спеціалістами: трудовий договір, договір цивільно-правового характеру (ЦПХ) та гіг-контракт. Гіг-контракт — правовий інструмент, що виявився справжнім проривом для ринку. А.Г. Тополь встановив, що на гіг-контракти припадає 72% усіх договірних відносин між резидентами Дія City та ІТ-спеціалістами станом на кінець 2024 року, тоді як частка класичних трудових договорів — лише 21% [14, С. 92].

Інвестиційна привабливість Дія City визначається не лише особливостями оподаткування праці фахівців, а й корпоративним податковим режимом. Резидент має право обрати між загальною системою оподаткування прибутку за ставкою 18% та спеціальним режимом податку на виведений капітал (ПнВК) за ставкою 9%. Принципова відмінність полягає в об'єкті оподаткування: класичний податок на прибуток справляється з фінансового результату незалежно від його подальшого використання, тоді як ПнВК сплачується лише в разі фактичного виведення капіталу — насамперед при виплаті дивідендів та прирівняних до них операціях. Поки прибуток реінвестується в розвиток компанії, податкове зобов'язання не виникає. Така конструкція є потужним стимулом до капіталізації ІТ-бізнесу й утримання прибутку всередині юрисдикції, що особливо цінно для стартапів на стадії зростання. Саме поєднання знижених ставок на оплату праці спеціалістів із відкладеним характером ПнВК формує ключову конкурентну перевагу режиму, яку в порівняльних оглядах нерідко згадують лише побіжно як «спеціальний податковий режим». Водночас слід урахувати перехідний характер окремих пільг: чинне законодавство передбачає поступове коригування податкових умов, тож довгострокове планування потребує врахування ризику зміни параметрів режиму впродовж життєвого циклу компанії.

У маркетинговому вимірі режим Дія City доцільно розглядати не лише як набір податкових пільг, а як інструмент позиціонування України у форматі національного брендингу (nation branding) — просування держави як інноваційного хабу з передбачуваними правилами гри. Поєднання гіг-контрактів, на які припадає 72% договірних відносин, із податком на виведений капітал за ставкою 9% утворює унікальну торгову пропозицію (USP) української юрисдикції: іноземний замовник отримує нижчу вартість розробки при збереженні високої якості послуг, а резидент — легальний і прозорий механізм оптимізації витрат. Саме така конфігурація

перетворює правовий режим на аргумент продажів у переговорах із глобальними клієнтами.

Таблиця 4

Динаміка резидентів Дія City (2022–2024 рр.)

Показник	I кв. 2022	IV кв. 2022	IV кв. 2023	IV кв. 2024
Кількість резидентів, од.	72	311	863	1 287
Кількість фахівців, тис. осіб	6,4	22,1	56,8	84,3
Середня зарплата, EUR/міс.	н/д	2 100	2 340	2 510
Частка гіг-контрактів, %	н/д	61	68	72
Залучені інвестиції, млн USD	н/д	210	480	740

Джерело: складено авторами за даними Міністерства цифрової трансформації України [1].

Таблиця 5

Порівняльний аналіз правових форм залучення ІТ-спеціалістів у режимі Дія City

Критерій	Трудовий договір	Договір ЦПХ	Гіг-контракт
Мінімальна оплата	≥ мінімальна зарплата (8 000 грн)	Договірна	≥ 1 200 EUR/міс.
Відпустка	24 робочих дні	Не передбачена	≥ 17 робочих днів
Лікарняні	Так (ФССУ)	Ні	Так (за рахунок компанії)
ПДФО + ВЗ	18% + 1,5%	5% (ФОП 3-я гр.) + 1,5%	5% + 1,5%
ЄСВ роботодавця	22% від зарплати	22% (часто оптимізують)	Не нараховується
Захист від звільнення	Повний (КЗпП)	Немає	Частковий (ст. 27 ЗУ)
Оптимальний для	Менеджерів, адмін. персоналу	Разових підрядників	Core ІТ-спеціалістів

Джерело: складено авторами за Законом України «Про стимулювання розвитку цифрової економіки в Україні» [13].

Порівняння трьох форм свідчить, що гіг-контракт оптимізований під потреби ІТ-ринку: відсутність ЄСВ-навантаження на компанію поєднується з прийнятним рівнем соціальних гарантій для фахівця. Проте О.В. Марченко фіксує два системних ризики: «псевдогігізацію» — переведення фактичних штатних працівників на гіг-контракти без надання реальної автономії, та нівелювання захисних норм в умовах воєнного стану — коли мораторій на перевірки фактично відступав перед розширеним колом контролюючих суб'єктів [12, С. 44].

Окремим, проте критично важливим виміром функціонування режиму Дія City в умовах воєнного стану стало мобілізаційне законодавство, зокрема механізм бронювання військовозобов'язаних. Право на бронювання працівників відповідно до постанови Кабінету Міністрів України від 5 червня 2024 р. № 650 «Деякі питання бронювання військовозобов'язаних під час воєнного стану» отримують підприємства,

визнані критично важливими для функціонування економіки або для забезпечення потреб Збройних Сил. Для ІТ-сектору, що формує 4,7–5,1% ВВП і залишається ключовим джерелом валютних надходжень, збереження кадрового ядра набуло значення питання економічної безпеки держави. Водночас чинна модель породжує дві системні колізії. Перша має суб'єктний характер: право на бронювання поширюється на штатних працівників, але не охоплює фахівців, залучених за гіг-контрактами та договорами ЦПХ, — попри те, що саме гіг-контракт законодавець позиціонував як основну форму взаємодії в Дія City (на нього припадає 72% договірних відносин). Виникає парадокс, за якого правовий інструмент, спеціально створений для ІТ-галузі, опиняється поза захисним полем мобілізаційного законодавства. Друга колізія є аксіологічною: держава одночасно прагне максимально мобілізувати людський ресурс для оборони та зберегти експортний потенціал галузі, що сама ж оборона фінансово підтримує. Підвищення з 10 червня 2025 р. зарплатного порогу для бронювання до 25 941 грн дещо звузило коло потенційних бенефіціарів, однак для ІТ-компаній із притаманним їм рівнем винагороди цей крок виявився радше формальним. Усунення зазначених колізій потребує узгодження критеріїв «критичної важливості» зі специфікою ІТ-зайнятості, насамперед — поширення механізму бронювання на гіг-спеціалістів резидентів Дія City.

Регулювання у сфері захисту персональних даних в Україні базується передовсім на Законі «Про захист персональних даних» 2010 року та Конвенції 108 Ради Європи. Водночас де-факто ще одним джерелом регуляторних вимог виступає GDPR — Регламент ЄС 2016/679, оскільки більшість великих українських ІТ-компаній обробляють дані громадян ЄС і зобов'язані дотримуватися його вимог екстратериторіально. О.В. Карпенко констатує: станом на 2024 рік Україна перебуває у стані «подвійного регуляторного навантаження» — вітчизняне законодавство та GDPR співіснують паралельно без повноцінного механізму уніфікації [15, С. 33].

Таблиця 6

Порівняння ЗУ «Про захист персональних даних» і GDPR

Параметр порівняння	ЗУ «Про захист ПД» (Україна)	GDPR (ЄС)
Рік прийняття / набрання чинності	2010 (ост. зміни — 2022)	2016 / 2018
Незалежний регулятор	Уповноважений ВРУ з прав людини	Незалежні DPA кожної держави-члена
Максимальний штраф	До 51 000 грн	До 20 млн EUR або 4% глоб. обороту
Право на забуття	Частково закріплено	Повністю закріплено (ст. 17)
Строк повідомлення про витік	Не встановлено	72 години від виявлення
Відповідальний за захист ПД (DPO)	Не вимагається	Вимагається для окремих категорій
Транскордонна передача даних	Нечіткий механізм	Standard Contractual Clauses (SCC), GDPR розд. V
Права суб'єктів	7 прав	8 прав (+ право на переносимість)
Підстави обробки ПД	3 підстави	6 підстав (згода, договір, юрид. зобов'язання та ін.)

Джерело: складено авторами за офіційними текстами законодавства України та Регламенту ЄС 2016/679.

Ця таблиця наочно демонструє, що вітчизняне законодавство про захист ПД поступається GDPR передусім у трьох вимірах: санкційна строгість, інституційна незалежність регулятора та операційні стандарти. Різниця у штрафних разюча: до 51 000 грн (~1 200 євро) проти 20 млн євро — тобто мінімум у 16 000 разів менше. За таких умов реальне дотримання вітчизняного закону про ПД виглядає радше доброю практикою, аніж вимушеним обов'язком для великих операторів.

Наведений розрив має безпосередній маркетинговий вимір: просування цифрових послуг на міжнародні ринки неможливе без довіри замовника до безпеки даних. За оцінкою В. М. Кравченка, створення незалежного регулятора персональних даних та впровадження 72-годинного строку повідомлення про витоки здатне збільшити обсяги аутсорсингових контрактів на 15–20% [21, С. 44] — прямий доказ того, що правова реформа функціонує як маркетинговий інструмент, конвертуючи регуляторну довіру у вимірюване зростання експорту.

Паралельно з захистом даних розвивалося кібербезпекове законодавство. Закон «Про основні засади забезпечення кібербезпеки України» (2017) встановив систему захисту критичної інформаційної інфраструктури (КІІ), визначив повноваження ДССЗІ та Держспецзв'язку, запровадив поняття кіберінциденту. В умовах повномасштабного вторгнення 2022–2024 роки стали найінтенсивнішим реальним тестуванням цих норм.

Таблиця 7

Статистика кіберінцидентів в Україні, зафіксованих CERT-UA (2021–2024 рр.)

Показник	2021	2022	2023	2024	Зміна 23/24, %
Загальна кількість інцидентів	1 438	2 194	1 988	2 543	+27,9
У т. ч. проти об'єктів КІІ	312	641	503	712	+41,5
Успішних атак на держсектор	98	187	142	203	+42,9
Атак на ІТ-компанії (комерц.)	215	387	341	422	+23,7
Залучено реагувань CERT-UA	1 438	2 194	1 988	2 543	+27,9

Джерело: складено авторами за звітами CERT-UA та Держспецзв'язку України [16]

Наведені дані свідчать про стабільно зростаючий рівень кіберзагроз: у 2024 році кількість кіберінцидентів зросла на 27,9% порівняно з 2023-м, причому атаки проти об'єктів критичної інфраструктури — на 41,5%. Це засвідчує, що чинне законодавство у сфері кібербезпеки, орієнтоване переважно на державний сектор, потребує термінового розширення на великий приватний бізнес — за прикладом директиви NIS2 ЄС.

Повномасштабна збройна агресія 2022–2024 років сформувала в Україні принципово новий сегмент ІТ-ринку — оборонні технології (MilTech). Екосистема Bravel, запущена у 2023 році як кластер оборонних технологій під спільним патронатом Міністерства цифрової трансформації, Міністерства оборони та Генерального штабу ЗСУ, функціонально інтегрована з режимом Дія City і станом на кінець 2024 року об'єднує понад 700 команд-розробників у сферах безпілотних

авіаційних систем, радіоелектронної боротьби, програмного забезпечення для управління полем бою та систем розвідки.

Попри практичну значущість, нормативно-правове поле для MilTech-стартапів залишається вкрай фрагментарним. По-перше, чинне законодавство про державні закупівлі (Закон України «Про публічні закупівлі» № 922-VIII) містить окремі спрощені процедури для оборонних потреб, однак не адаптоване до специфіки програмного забезпечення та цифрових сервісів, де цикл розробки та верифікації є принципово коротшим, ніж для традиційних озброєнь. По-друге, питання права інтелектуальної власності при державних закупівлях ІТ-рішень для оборони залишається законодавчо неврегульованим: чинна практика передбачає, як правило, повну передачу майнових прав на розроблені рішення державі, що позбавляє стартапи можливості комерціалізувати технологію на ринках союзників. По-третє, сертифікація програмних продуктів оборонного призначення здійснюється за загальними вимогами технічного захисту інформації ДССЗІ, розробленими переважно для класичних інформаційних систем і недостатньо адаптованими до специфіки вбудованого програмного забезпечення, систем реального часу та AI-асистованих рішень. Усунення зазначених прогалин є передумовою перетворення України на повноцінний центр оборонних технологій із конкурентоздатною правовою базою.

Поглиблення аналізу MilTech-сегмента потребує окремої уваги до режиму експортного контролю програмного забезпечення подвійного призначення. Оборонні ІТ-рішення — від систем управління полем бою до платформ радіоелектронної боротьби — за своєю природою належать до товарів, передача яких за кордон підпадає під дію законодавства про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання. Виникає суперечність між прагненням MilTech-стартапів масштабуватися на ринки держав-союзників і жорсткістю процедур експортного контролю, посилені в умовах війни. Особливо гостро ця суперечність постає для алгоритмів та моделей машинного навчання, нематеріальна природа яких ускладнює застосування класичних митних механізмів: фактичний «експорт» технології може відбутися шляхом надання віддаленого доступу до коду чи хмарного сервісу, що формально не перетинає кордону. Додаткової невизначеності додає правовий статус так званих цивільних розробників — фахівців і компаній, які створюють софт оборонного призначення поза межами офіційного оборонно-промислового комплексу. Чинне законодавство не дає однозначної відповіді на питання про обсяг їхніх зобов'язань у сфері експортного контролю, режиму секретності та відповідальності за подвійне використання продукту. Формування зрозумілих та передбачуваних правил експорту програмного забезпечення подвійного призначення, гармонізованих із підходами ЄС і НАТО, є необхідною умовою для того, щоб українські MilTech-рішення, апробовані в реальних бойових умовах, могли бути легально комерціалізовані на ринках партнерів.

У маркетинговій площині врегулювання експорту технологій подвійного призначення відкриває для українських MilTech-стартапів доступ до позиціонування «battle tested» — просування продуктів, що пройшли реальну апробацію в бойових умовах. Такий статус є рідкісною конкурентною перевагою на глобальному ринку оборонних технологій, адже жоден полігонний тест не замінює верифікації в умовах реального застосування. Легалізація комерціалізації подібних рішень на ринках союзників перетворить військовий досвід галузі на експортний актив.

Авторсько-правова охорона об'єктів ІТ-сфери в Україні регулюється Законом

«Про авторське право і суміжні права» у новій редакції 2022 року. Оновлений закон закріпив охорону комп'ютерних програм як літературних творів відповідно до Угоди TRIPS і Директиви ЄС 2009/24/ЄС, визначив особливості правового режиму баз даних, встановив правила щодо службових творів та спеціальні норми щодо цифрового розповсюдження. Попри це, практика застосування авторсько-правових норм у сфері ПЗ залишається проблематичною: В.В. Апалькова встановила, що середня тривалість розгляду справ про порушення авторських прав на ПЗ у судах першої інстанції у 2022–2023 роках становила 14,7 місяця [4, С. 56].

Таблиця 8

Об'єкти інтелектуальної власності ІТ-сфери та їхній правовий статус в Україні

Об'єкт ІВ	Форма охорони	Нормативна база	Тривалість охорони	Правові прогалини
Комп'ютерна програма	Авторське право	ЗУ «Про АП», ст. 8	Строк життя + 70 р.	Складне доведення порушення
База даних	АП / sui generis	ЗУ «Про АП», ст. 14	15 р. від створення	Нечіткі критерії оригінальності
Алгоритм	Не охороняється	—	—	Законодавча прогалина
Логотип / GUI	АП + знак для товарів	ЗУ «Про АП» + «Про охорону знаків»	Необмежено / 10 р. з поновл.	Розмежування ТМ та АП
Ноу-хау / Trade secret	Комерційна таємниця	ГКУ, ст. 36	Необмежено	Слабкий захист при розголошенні
АІ-генерований контент	Не охороняється	—	—	Повна законодавча прогалина
Доменне ім'я	Квазі-власність (договір)	—	Строк реєстрації	Відсутній спеціальний закон

Джерело: складено авторами за текстами законодавства України та матеріалами ДСІВ.

Наведена класифікація засвідчує структурну прогалину: сучасні ІТ-продукти — алгоритми, системи машинного навчання та АІ-генерований контент — залишаються поза системою формальної охорони. Ця ситуація відображає загальносвітову дискусію: ВОІВ лише у 2024 році опублікувала перші рекомендаційні документи щодо авторства штучного інтелекту, не надавши остаточної відповіді на питання про охороноздатність АІ-генерованих об'єктів [17, С. 34].

Євросоюз у 2022–2024 роках здійснив найамбітніший в історії цифрового права регуляторний прорив, запровадивши цілий пакет взаємопов'язаних інструментів, що у своїй сукупності формують Єдиний цифровий ринок (Digital Single Market). За підрахунками Єврокомісії, повне впровадження DSM здатне додати до ВВП ЄС від 415 до 500 млрд євро щорічно [18, С. 7]. Ця цифра задає вимірюваний орієнтир того, яку економічну цінність продукує ефективне регуляторне середовище — і наскільки велика ціна регуляторної інертності.

Центральними елементами регуляторного пакету ЄС виступають: Digital

Services Act (DSA, 2022), що встановлює ієрархічні зобов'язання для онлайн-платформ залежно від їхнього масштабу; Digital Markets Act (DMA, 2022), що визначає поняття «gatekeepers» (воротарів ринку) та встановлює для них спеціальні ex ante заборони самофаворизації; AI Act (2024) — перший у світі обов'язковий закон про штучний інтелект, що класифікує AI-системи за чотирма рівнями ризику (неприйнятний, високий, обмежений, мінімальний) та встановлює диференційовані вимоги до прозорості й аудиту; нарешті, GDPR (2016/2018) залишається наріжним каменем регулювання обробки персональних даних з екстратериторіальним ефектом [18, С. 15].

Таблиця 9

Регуляторні інструменти ЄС у сфері цифрової економіки (2022–2026 рр.)

Інструмент	Набрав чинності	Регулятивний механізм	Адресати	Санкції
GDPR (2016/679)	2018	Обробка персональних даних	Усі обробники ПД	До 4% глоб. обороту
Digital Services Act	2023 (повністю)	Відповідальність платформ	Онлайн-платформи, посередники	До 6% глоб. обороту
Digital Markets Act	2023	Конкуренція на цифрових ринках	Gatekeepers (Alphabet, Apple, Meta)	До 10% глоб. обороту
AI Act	2026 (повністю)	Регулювання ризиків ШІ	Розробники та провайдери AI	До 35 млн EUR або 7%
NIS2 Directive	2024	Кібербезпека критичних секторів	Оператори важливих послуг	До 10 млн EUR або 2%
Data Act	2025	Доступ до промислових даних	ІоТ-виробники, хмарні сервіси	До 4% глоб. обороту

Джерело: складено авторами за матеріалами Офіційного журналу ЄС (Official Journal of the EU) [18].

Аналіз пакету демонструє системний підхід: кожен регуляторний інструмент таргетований на конкретний ринковий провал. Принципово, що санкційна система ЄС побудована на прив'язці до глобального обороту, а не до фіксованих сум — що забезпечує ефективний вплив навіть на транснаціональних гравців із мільярдними доходами. Для порівняння: максимальний штраф за порушення українського закону про захист ПД становить 1 200 євро, тоді як штраф Google від CNIL (Франція) за порушення GDPR у 2022 році — 150 млн євро, тобто у 125 000 разів більше.

Три держави, що в різний спосіб досягли статусу глобальних ІТ-хабів — Естонія, Сінгапур та Ізраїль — послуговуються суттєво відмінними регуляторними стратегіями. Їхній досвід надає безцінний порівняльний матеріал для формування рекомендацій, придатних до адаптації в українських умовах.

Естонська модель (e-Estonia) базується на принципі «цифрового за замовчуванням» (digital by default): усі державні послуги надаються в електронній формі як основній. Правовою основою слугують Закон про електронну ідентифікацію (1999, ред. 2018), Закон про захист персональних даних (2007, адаптований до GDPR у 2018 р.) та Закон про кібербезпеку (2018). Естонія першою у світі запровадила систему електронного резидентства (e-Residency, 2014) та блокчейн-захист державних реєстрів (X-Road). Н.О. Рибачок та Л.Д. Тімченко встановили, що стабільність правил

гри упродовж понад двадцяти років — а не якийсь унікальний технологічний ресурс — є визначальним чинником успіху естонської цифрової держави [20, С. 78].

Естонський досвід e-Residency знайшов безпосереднє відображення у вітчизняній політиці: Законом України «Про внесення змін до Податкового кодексу України щодо особливостей оподаткування електронних резидентів (e-резидентів)» було запроваджено власний інститут електронного резидентства, а порядок набуття й скасування відповідного статусу та функціонування інформаційної системи «Е-резидент» урегульовано підзаконними актами 2022–2023 років. Е-резидент — це особливий статус іноземного громадянина, що дозволяє дистанційно, без фізичної присутності в Україні, заснувати бізнес, відкрити рахунок та сплачувати податки через єдину онлайн-систему. Подібно до естонської моделі, статус недоступний громадянам держави-агресора та країн «сірого» і «чорного» списків FATF. Попри концептуальну привабливість, український проєкт демонструє типову для вітчизняного нормотворення ваду: тривалий розрив між ухваленням рамкового закону та запуском повноцінно дієздатної інформаційної інфраструктури. На відміну від Естонії, де e-Residency від початку інтегрувалося в зрілу екосистему X-Road, українська система розгорталася поетапно й тривалий час перебувала у стані тестування. Стратегічна цінність інституту полягає в його потенціалі залучати закордонних ІТ-підприємців до української юрисдикції в умовах глобальної конкуренції за таланти, у якій Україна змагається не лише з Естонією, а й із Сінгапуром. Реалізація цього потенціалу прямо залежить від синхронізації e-резидентства з режимом Дія City та від правової визначеності щодо транскордонного руху коштів e-резидентів.

Сінгапурська модель орієнтована на залучення глобальних ІТ-інвестицій через поєднання жорсткого захисту інтелектуальної власності, сприятливого корпоративного оподаткування та передбачуваної правової системи common law. Закон про захист персональних даних (PDPA, 2012, ред. 2021) вирізняється специфічним балансуванням між правами суб'єктів ПД та бізнес-інтересами: до 2021 року він не передбачав обов'язку повідомлення про витоки, натомість від 2021 року встановив 3-денний строк — суворіший за GDPR. Ізраїльська модель характеризується особливою увагою до кіберрегулювання, що є закономірним для держави, де кіберзахист набуває виміру національної безпеки. Ізраїльське Національне кіберуправління (INCD) поєднує функції регулятора та оперативного органу реагування, встановлюючи обов'язкові галузеві кіберстандарти для фінансових установ, охорони здоров'я та комунікаційної інфраструктури.

Узагальнення досвіду ЄС, Естонії, Сінгапуру та Ізраїлю дозволяє виокремити три принципи ефективного регулювання ІТ-галузі, що не залежать від розміру держави чи її геополітичного контексту. Перший — регуляторна передбачуваність: ІТ-компанії планують діяльність лише за умови стабільності правових норм щонайменше на три–п'ять років. Другий — пропорційність регулювання: найефективніші системи диференціюють регуляторне навантаження залежно від розміру компанії та рівня ризику діяльності. Третій — багаторівневий інституційний дизайн: жодна з аналізованих систем не зосереджує регуляторні функції в одному органі [19, С. 88].

Таблиця 10

Порівняльний аналіз регуляторних моделей ІТ-галузі (ЄС, Естонія, Сінгапур, Ізраїль, Україна)

Параметр	ЄС	Естонія	Сінгапур	Ізраїль	Україна
Єдиний цифровий закон	Частково (DSA/DMA)	Система законів	Система законів	Система законів	Відсутній
Спецрежим для ІТ	Немає	Загальний бізнес-клімат	Global Investor Programme	Start-Up Nation	Дія City
Незалежний регулятор ПД	DPA (кожна держава)	АКІТ	PDPC	PPA	Уповноважений ВРУ (слабкий)
Строк повід. про витік	72 год.	72 год. (GDPR)	3 доби	72 год.	Не встановлено
Закон про ШІ	AI Act (2026)	AI Act (відповідно)	Soft law framework	Draft (2024)	Відсутній
Кіберрегулятор	ENISA + нац. органи	RIA	CSA	INCD	ДССЗЗІ / Держспецзв'язок
Рейтинг ITU GCI (2024)	—	7-ме місце	4-те місце	11-те місце	25-те місце
Максимальний штраф за порушення ПД	20 млн EUR / 4%	20 млн EUR (GDPR)	1 млн SGD	3,36 млн USD	~1 200 EUR

Джерело: складено авторами за даними ITU Global Cybersecurity Index 2024, OECD Digital Economy Outlook 2024 [19].

Зіставлення п'яти регуляторних моделей у таблиці 10 виявляє, що відставання України має не точковий, а системний характер: за жодним із восьми параметрів вітчизняна система не досягає рівня держав-орієнтирів. Особливо показовою є кореляція між інституційною незалежністю регулятора персональних даних і позицією в рейтингу ITU GCI — Естонія, Сінгапур та Ізраїль, що мають самостійні наглядові органи (АКІТ, PDPC, PPA), посідають відповідно 7-ме, 4-те та 11-те місця, тоді як Україна з функціонально залежним Уповноваженим Верховної Ради опинилася на 25-й позиції. Не менш промовистим є розрив у санкційному вимірі: гранична межа штрафу в Україні (близько 1 200 євро) є непорівнянною навіть із сінгапурським показником (1 млн SGD), не кажучи вже про загальноєвропейські 20 млн євро. Водночас наявність власного спеціального режиму Дія City — параметр, за яким Україна випереджає більшість аналізованих юрисдикцій, — свідчить, що проблема полягає не у відсутності правових інструментів як таких, а у фрагментарності інституційного забезпечення та м'якості примусових механізмів. Саме цей висновок і визначає логіку матриці реформ, наведеної далі. У бенчмаркінговому вимірі наведене зіставлення окреслює маркетинговий потенціал України як цифрової нації: за умови інституційної розбудови держава з 25-м місцем у рейтингу ITU GCI має реалістичні шанси наблизитися до лідерів — Естонії (7-ме місце) та Сінгапуру (4-те), — що безпосередньо підвищить її позиції у сприйнятті глобальних замовників цифрових послуг.

**Матриця рекомендацій щодо вдосконалення нормативно-правового
регулювання ІТ-галузі України**

№	Напрямок реформи	Нинішній стан	Рекомендований захід	Пріоритет	Строк
1	Регулювання штучного інтелекту	Правова порожнеча	Закон «Про штучний інтелект» (гармон. з AI Act ЄС)	Критичний	2025–2026
2	Незалежність регулятора ПД	Уповноважений ВРУ — залежний	Незалежний ДПА з бюджетною автономією	Критичний	2025
3	Повідомлення про витоки ПД	Строк не встановлено	72-годинний строк (GDPR-стандарт)	Високий	2025
4	Транскордонна передача даних	Нечіткий механізм	Запровадити SCC (Standard Contractual Clauses)	Високий	2025–2026
5	Охорона AI-контенту	Правова порожнеча	Визначити правовий статус AI-авторства у ЗУ «Про АП»	Середній	2026
6	Кіберстандарти для бізнесу	Лише держсектор	Поширити обов'язк. стандарти на великий бізнес (NIS2)	Високий	2025–2026
7	Судовий захист ІВ в ІТ	Повільний (14,7 міс.)	Спеціалізована палата з ІТ-спорів	Середній	2026–2027
8	Критерії входу до Дія City	Зростаючий бар'єр (EUR)	Знизити вхідний поріг для регіональних ІТ-компаній	Середній	2025

Джерело: складено авторами на основі порівняльного аналізу регуляторних моделей.

Рекомендація щодо створення спеціалізованої ІТ-юрисдикції потребує конкретизації організаційної моделі. Нині в Україні існує прецедент спеціалізованого судочинства у сфері інтелектуальної власності — Вищий суд з питань інтелектуальної власності, що формально утворений і розпочав роботу у 2021 році, однак досі функціонує зі значними процесуальними обмеженнями та дефіцитом суддів із технічною експертизою. Цей досвід, зокрема труднощі з формуванням корпусу суддів, здатних кваліфіковано оцінювати технологічні додокази, є важливим застереженням для проектування нової установи.

Аналіз зарубіжного досвіду дозволяє виокремити дві реалістичні моделі. Перша — окрема спеціалізована палата з ІТ-спорів у межах Господарського суду міста Київ за аналогією з практикою Сінгапуру, де Singapore International Commercial Court (SICC) розглядає складні транскордонні комерційні спори, включаючи технологічні, із залученням іноземних суддів і застосуванням принципів common law. Ця модель вирізняється гнучкістю та дозволяє концентрувати технічну експертизу без повної реорганізації судової системи. Друга модель — окремий спеціалізований суд за

зразком Bundespatentgericht (Федерального патентного суду Німеччини) — потребує значно більших інституційних та фінансових ресурсів і доцільна лише у повоєнній перспективі. З урахуванням реалістичних часових горизонтів реформи пріоритетною видається перша модель із поступовим розширенням юрисдикції та підготовкою суддів за спільними програмами з EUIPO та ENISA.

З погляду маркетингу цифрових послуг спеціалізоване правосуддя виконує функцію «гарантійного талона» для іноземного інвестора: наявність швидкого та професійного суду за сінгапурським зразком сигналізує, що права інтелектуальної власності будуть захищені не за 14,7 місяця, а у значно стисліші строки. Передбачуваність судового захисту знижує премію за ризик, яку інвестори закладають у вартість капіталу для української юрисдикції.

Практичне впровадження зазначених рекомендацій передбачає не тільки законодавчі зміни, а й серйозне інституційне будівництво. За підрахунками В.М. Кравченка, лише впровадження незалежного DPA та 72-годинного строку повідомлення про витоки здатне підвищити рівень довіри ЄС-партнерів до українських ІТ-компаній і збільшити обсяги аутсорсингових контрактів орієнтовно на 15–20% [21, С. 44].

Переходячи від рекомендацій до перспективи: Україна у повоєнній відбудові матиме унікальний шанс здійснити цифровий стрибок уперед, поєднавши функціональний Дія City з AI Act-сумісним законодавством та незалежною регуляторною архітектурою. Саме такий шлях пройшла Естонія у 1990-х роках, будуючи цифрову державу фактично з нуля — і ставши еталонною «цифровою нацією» вже на початку 2000-х.

Висновки. Проведений аналіз нормативно-правового регулювання ІТ-галузі в Україні та порівняльне дослідження міжнародного досвіду дозволяють сформулювати чотири системних висновки.

По-перше, чинна нормативна база ІТ-сектору України — близько двадцяти спеціальних законів без єдиного кодифікованого акту — є внутрішньо суперечливою системою з виразними прогалинами у регулюванні штучного інтелекту, транскордонної передачі даних та AI-авторства. Ані рамкового закону про ІІІ, ані закону про цифрові ринки, ані законодавства про ІоТ Україна досі не має. Переговорний процес про вступ до ЄС фактично робить ці акти неминучими у горизонті 2026–2028 років.

По-друге, режим Дія City продемонстрував вимірювану ефективність: за три роки (2022–2024) кількість резидентів зросла з 72 до 1 287 компаній, сукупний персонал перевищив 84 000 фахівців, середня заробітна плата досягла 2 510 євро на місяць. Водночас практика виявила системні вразливості: «псевдогігізацію», фактичне нівелювання захисту від перевірок в умовах воєнного стану та зростання вхідного бар'єру через валютну динаміку. Окремим напрямом, що набуватиме дедалі більшого значення в контексті євроінтеграції, є запровадження ESG-критеріїв (Environmental, Social, and Governance) у регулювання резидентів Дія City. Директива ЄС про корпоративну звітність зі сталого розвитку (CSRD, 2022/2464) поширюється на великі компанії, що мають цінні папери, допущені до торгів на регульованих ринках ЄС, та на підприємства, що відповідають двом із трьох порогових критеріїв за чисельністю персоналу, оборотом і активами. У міру того як українські ІТ-компанії виходять на ринки ЄС, залучають євроінвесторів і прагнуть лістингу на європейських біржах, вимоги CSRD ставатимуть для них практично обов'язковими.

Конкретно для ІТ-сектору це означає насамперед звітність щодо

енергоспоживання та вуглецевого сліду дата-центрів: відповідно до Акту про енергоефективність ЄС (Energy Efficiency Directive, 2023/1791), дата-центри потужністю понад 500 кВт із 2024 року зобов'язані розкривати показники ефективності використання електроенергії (PUE) та відновлюваної енергії (REF). Попри те що Україна поки не є членом ЄС, включення ESG-вимог до критеріїв резидентства Дія City — хоча б у добровільному форматі як стандарт «найкращої практики» — значно посилить конкурентоздатність українських ІТ-компаній при виході на ринки ЄС і полегшить залучення інвестицій від ESG-орієнтованих фондів. У маркетинговому контексті відповідність ESG-нормам виконує роль «перепустки» на ринки ЄС: розкриття вуглецевого сліду дата-центрів та звітність за CSRD стають обов'язковою умовою залучення євроінвесторів і лістингу на європейських біржах, перетворюючи комплаєнс на складову маркетингового просування компанії.

По-третє, зіставлення з моделями ЄС, Естонії (7-ме місце ITU GCI), Сінгапуру (4-те місце) та Ізраїлю (11-те місце) засвідчує: Україна (25-те місце) відстає передусім в інституційному вимірі — незалежність регулятора персональних даних, наявність законодавства про ШІ та строгість кіберзахисних стандартів для приватного сектору. Різниця у максимальних санкціях за порушення у сфері захисту ПД — 1 200 євро в Україні проти 20 млн євро в ЄС — унаочнює слабкість вітчизняних примусових механізмів.

По-четверте, впровадження восьми рекомендованих реформ — від Закону про штучний інтелект до спеціалізованої ІТ-юрисдикції та незалежного ДРА — потребує насамперед інституційного будівництва та навчання кадрів регуляторних органів і судової системи. Саме інституційна слабкість регуляторів, а не дефіцит правових норм, є визначальним гальмом розвитку правового середовища ІТ-галузі. Ефективна реалізація зазначених реформ здатна збільшити обсяги ІТ-експорту на 15–20% та суттєво прискорити процес євроінтеграції у цифровій сфері.

Узагальнюючи, описані правові реформи слід розглядати як фундамент реалізації маркетингової стратегії просування українських ІТ-послуг на глобальному ринку: вони формують довіру міжнародних замовників, знижують юрисдикційні та безпекові ризики і створюють цінову привабливість галузі. Інституційна розбудова регуляторного середовища відтак постає не лише умовою євроінтеграції, а й прямим чинником зростання експортної конкурентоздатності України як цифрової нації.

Перспективи подальших наукових розвідок у цьому напрямі пов'язані з дослідженням механізмів імплементації вимог EU AI Act у діяльність українських ІТ-компаній, розробленням правового режиму смарт-контрактів у вітчизняному цивільному законодавстві, оцінюванням ефективності запровадження ESG-критеріїв у режим Дія City, а також моніторингом результативності запропонованих реформ у міру просування переговорного процесу про вступ України до ЄС.

Список використаної літератури:

1. Апалькова В. В., Грищенко І. М. Цифрова економіка та правовий захист у сфері авторського права ІТ. Вісник економіки. 2023. № 2. С. 28–62.
2. Асоціація IT Ukraine. Аналітичний звіт: ІТ-галузь України у 2023 році. Київ, 2024. 64 с.
3. Вишневецький О. С. Цифрова трансформація суспільства: правовий вимір : монографія. Київ : НАН України, 2023. 284 с.
4. Гаращенко Л. П. Гіг-контракти в ІТ-секторі: правова природа та практика застосування. Право України. 2023. № 6. С. 60–74.

5. Державна служба спеціального зв'язку та захисту інформації України (CERT-UA). Звіт про кіберінциденти в Україні у 2024 році. Київ, 2025. 78 с. URL: <https://cert.gov.ua/article/reports>
6. Закон України «Про стимулювання розвитку цифрової економіки в Україні» від 15.07.2021 № 1667-IX. Відомості Верховної Ради України. 2021. № 41. Ст. 326.
7. Карпенко О. В. Подвійне регуляторне навантаження: ЗУ «Про захист ПД» та GDPR у діяльності ІТ-компаній. Інформація і право. 2024. № 2. С. 28–41.
8. Кравченко В. М. Регуляторний потенціал незалежного наглядового органу у сфері захисту персональних даних. Цифрова Україна: стратегічне бачення. 2024. № 1. С. 38–52.
9. Краус Н. М., Краус К. М. Дія City як інноваційна правова платформа цифрової економіки: переваги та обмеження. Бізнес-Інформ. 2023. № 4. С. 72–89.
10. Ляшенко В. І., Вишневська О. А. Правові виміри цифрової індустріалізації в Україні. Економіка промисловості. 2022. № 4. С. 105–121.
11. Марченко О. В. Захист від перевірок в умовах воєнного стану: колізії законодавства. Юридична Україна. 2024. № 2. С. 38–51.
12. Міністерство цифрової трансформації України. Звіт про стан розвитку цифрової економіки та Дія City у 2024 році. Київ : Мінцифри, 2024. 96 с. URL: <https://www.mintsifry.gov.ua>
13. Пилипенко Г. М. Еволюція парадигм регулювання цифрової економіки. Науковий вісник Дніпровського ДАЕУ. 2023. № 1. С. 50–64.
14. Тімченко Л. Д., Рибачок Н. О. Естонська модель е-урядування як орієнтир для України. Публічне управління та адміністрування в Україні. 2023. № 31. С. 72–84.
15. Тополь А. Г. Ризики псевдогігізації в ІТ-секторі України: трудово-правовий аналіз. Часопис Київського університету права. 2024. № 1. С. 88–98.
16. Харченко В. В., Карпенко О. В. Термінологічна визначеність у законодавстві про інформаційні технології. Правова держава. 2022. № 33. С. 18–30.
17. Чорна О. В. Правові форми залучення ІТ-фахівців: від трудового договору до гіг-контракту. Підприємство, господарство і право. 2023. № 8. С. 82–96.
18. European Commission. The Digital Decade Policy Programme 2030: Economic Impact Assessment. Luxembourg : Publications Office of the EU, 2023. 134 p.
19. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review. 2022. Vol. 1. P. 72–89.
20. OECD. OECD Digital Economy Outlook 2024: Shaping Technologies for an Open, Trustworthy and Sustainable Digital Future. Paris : OECD Publishing, 2024. 246 p.
21. World Intellectual Property Organization (WIPO). Generative AI and Intellectual Property: A Policy Discussion Paper. Geneva : WIPO, 2024. 102 p.

Дата надходження статті: 17.08.2026

Дата прийняття статті: 07.09.2026

Дата публікації статті: 30.09.2026