УДК 34.05:004.738.5:342.7:339.13

DOI: https://doi.org/10.32782/2520-2200/2025-4-1

Дехтяр Н.А.
кандидат економічних наук, доцент,
доцент кафедри міжнародної економіки і менеджменту
Харківського національного економічного університету
імені Семена Кузнеця
Снопченко М.Ю.
викладач кафедри міжнародної економіки і менеджменту
Харківського національного економічного університету
імені Семена Кузнеця

Dekhtyar Nadiya, Snopchenko Milana
Simon Kuznets Kharkiv National University of Economics

МОДЕРНІЗАЦІЯ ЦИФРОВОГО ЗАКОНОДАВСТВА ЄС З МЕТОЮ ЗАХИСТУ ПРАВ КОРИСТУВАЧІВ ТА РЕГУЛЮВАННЯ РИНКУ ЦИФРОВИХ ПОСЛУГ[1]

MODERNISATION OF EU DIGITAL LEGISLATION TO PROTECT USER RIGHTS AND REGULATE THE DIGITAL SERVICES MARKET

Стаття аналізує нормативну еволюцію цифрового регулювання ЄС, починаючи з GDPR та його доповнення документами DSA, DMA, DGA і Data Act. Розглянуто, як ці закони та регламенти формують багаторівневу систему управління даними, забезпечують прозорість, конкуренцію, захист прав користувачів і доступ до даних. Особлива увага приділена екстериторіальності, взаємодії персональних і неперсональних даних, а також ролі Європейської комісії. Підкреслено, що нова архітектура цифрового регулювання змінює вимоги до платформ, інструментів та процедур, вимагаючи адаптації до сучасного цифрового середовища. Додатково розглядаються вимоги щодо сплати ПДВ для підприємств, що надають цифрові послуги споживачам у ЄС, аналізуються регуляторні положення, які стосуються як резидентів, так і нерезидентів ЄС, зокрема українських компаній, що експортують цифрові продукти – програмне забезпечення, онлайн-курси, потокові сервіси, хмарні обчислення та ін.

Ключові слова: цифрові ринки, експорт IT-послуг до ЄС, законодавче регулювання електронної торгівлі, кібербезпека, ПДВ в торгівлі цифровими послугами.

The article provides a comprehensive analysis of the transformation of the European Union's regulatory framework in the field of digital regulation. It starts with the General Data Protection Regulation (GDPR) – despite its systematic nature, this document did not cover all the challenges arising from the rapid development of digital technologies. In response to new risks and needs, the EU has developed a series of supplementary regulations that detail and expand upon the GDPR's provisions, forming a multi-level architecture of digital governance. Notably, the Digital Services Act (DSA) establishes requirements for online platforms concerning content moderation, algorithm transparency, safeguarding user rights and granting access to data for research purposes. The Digital Markets Act (DMA) aims to limit the dominance of 'gatekeepers' – large technology companies that control access to key digital services – by introducing mandatory competition, transparency and interoperability rules. The Data Governance Act (DGA) establishes a foundation for a single data market by promoting the reuse of public sector

[1] Спільне фінансування від Європейського Союзу. Підготовлено в рамках проекту "101098892 — DigiTrade. EU4UA — ERASMUS-JMO-2022-HEI-TCH-RSCH-UA-IBA / ERASMUS-JMO-2022-HEI-TCH-RSCH". Висловлені погляди та думки є виключно поглядами та думками авторів і не обов'язково відображають позицію Європейського Союзу. Європейський Союз та орган, що надає грант, не несуть відповідальності за них.

data, developing intermediary services and encouraging altruism within the data sphere. The Data Act ensures fair access to data generated by connected devices and establishes control mechanisms, intellectual property protection and confidentiality regulations for data exchange between private and public entities. All of these acts have extraterritorial effect, cover both personal and non-personal data, and interact with the GDPR to create a horizontal regulatory system for the digital economy. Additionally, the article discusses the current VAT payment requirements for companies providing digital services to EU consumers. It provides an overview of the relevant regulations for both EU and non-EU residents that export digital products such as software, online courses, streaming services, and cloud computing. Special attention is paid to the taxation specifics for Ukrainian companies, including the registration requirements for non-residents in Ukraine and the exemption of B2B services from Ukrainian VAT. It also suggests practical recommendations for Ukrainian exporters on how to comply with tax regulations, keep records and adapt to European regulatory changes in the field of digital trade. In conclusion, this article shows how regulatory convergence within the EU is changing the way data is managed and how digital services and markets operate. This requires tools, procedures and terminology to be adapted by Ukrainian IT-companies to ensure compliance with modern digital requirements.

Keywords: digital markets, export of IT services to the EU, legislative regulation of e-commerce, cybersecurity, VAT in trade in digital services.

Постановка проблеми. Упродовж останніх п'яти років в законодавстві ЄС відбувалися серйозні зміни щодо регулювання цифрової економіки, зокрема встановлювалися нові правила й обмеження на діяльність крупних гравців цифрового ринку, політики управління даними користувачів, підсилювалися заходи з кібербезпеки. Європейський онлайн-ринок є привабливим для українських підприємств, багато IT-компаній вже мають значний досвід співпраці як з індивідуальними користувачами, так і корпоративними клієнтами. Стратегічним завданням є підтримка національних підприємств і стартапів, які мають на меті розширювати географію діяльності і виходити на нові для себе напрямки. У самих країнах ЄС зростає попит на IT-фахівців, наприклад, у 2023 р. майже 5% зайнятих (близько 10 млн. осіб) працювали у галузі IT, 20% усіх фізичних товарів були придбані приватними особами онлайн, 50% підприємств використовували те чи інше програмне забезпечення для автоматизації бізнес-процесів (ERP, CRM чи BI), 20,75% підприємств отримали замовлення через засоби електронної торгівлі в обсязі не менше 1% від річного обороту; у 2024 р. 13,48% підприємств із кількістю найманих працівників понад 10 осіб і 41,18% підприємств із понад 250 працівниками використовували штучний інтелект [1]. Із зростанням обсягів торгівлі фізичними товарами через Інтернет і розширенням асортименту цифрових продуктів посилюватиметься державний контроль за надавачами електронних послуг. На сьогодні найбільше викликів провокують транскордонні операції – окрім суто технічного завдання із моніторингу інформаційних потоків через кордони країн, постає питання узгодження законодавчих способів регулювання подання звітності, сплати податків, збереження даних користувачів компаніями, які працюють у глобальній мережі. Перед законодавцями постає дилема, як зберегти прозорість національного ринку, справедливий рівень вільної конкуренції і низькі бар'єри входу для кваліфікованих фахівців і якісної продукції й водночас мінімізувати хаос і побудувати належну систему контролю, без якої на ринок можуть зайти шахраї і відверто неетичні гравці. За декількома ініціативами ЄС є першим у світі, і заздалегідь знаючи правила гри, українські IT-розробники зможуть долучитися до прибуткового європейського ринку.

Аналіз останніх досліджень та публікацій. Аналіз чинного законодавства ЄС у галузі цифрової економіки міститься у роботах А. Флетчер та ін. [2] – як Закон про цифрові ринки корелює із загальноекномічною доктриною на прикладі роботи великих онлайн-платформ, С. Хайдебрехт [3] оцінює політику єдиного цифрового ринку (DSM) та її вплив на свободу цифрового підприємництва, Є. Шмідт та ін. [4] аналізують законодавство у сфері штучного інтелекту, Т. Шарон і Р. Геллерт [5] – спроби ЄС зменшити негативний вплив BigTech – найкрупніших IT-корпорацій світу, Ф. Вліст та ін. [6] розглядають феномен «надзастосунку» (super-app) та вплив таких розробок на глобальний ринок. Багато публікацій присвячені регулюванню цифрових фінансових ринків та використання криптовалюти, але це – великий окремий напрямок досліджень, якого ми у даній статті торкатися не будемо. Зазначимо, що у порівнянні з іншими темами, в останні два–три роки не так багато європейських вчених займалися проблематикою цифрового законодавства – навпаки, ця тема є дуже популярною в українських науковців, ймовірно, з причини геополітичного спрямування економіки України на ринок ЄС. У межах нашого дослідження відмітимо роботи І. П. Васильчук та К. В. Слюсаренко [7], С. Іванцова [8], І. В. Ковбаса та О. М. Редько [9], Л. О. Шворак та Я. О. Гуменюка [10], які розглядали різні аспекти інтеграції українських компаній у цифровий простір ЄС. Отже, ця тема є сьогодні достатньо актуальною,

і, незважаючи на велику кількість джерел, що освітлюють дану проблематику, варто проаналізувати вплив останніх нормативних документів у сукупності, адже, починаючи з 2022 року, їхній перелік суттєво розширився.

Метою статті є огляд законодавства Європейського Союзу у галузі цифрових послуг, роз'яснення правил та процедур, яких повинні дотримуватися українські розробники, пропонуючи свій продукт на експорт. Основну увагу буде приділено таким нормативно-правовим документам, як: Загальний регламент про захист даних (GDPR), Закон про цифрові послуги (DSA), Закон про цифрові ринки (DMA), Закон про управління даними (DGA), Закон про дані (DA), Директива про мережеві та інформаційні системи (NIS2), Закон про кіберстійкість (CRA), Закон про штучний інтелект (AI Act), а також будуть розглянуті деякі питання стосовно ПДВ та оподаткування цифрових послуг.

Виклад основного матеріалу дослідження. Розглянемо завдання основних нормативних документів, з точки зору їхньої корисності для кінцевих користувачів та часткових або повних обмежень, які вони накладають на розробників та постачальників, якщо порівнювати із практиками того часу, коли ці регламенти ще не вступали в дію. Зрозуміло, що на етапі впровадження та «налаштування» вимог законодавчих актів під реальну ситуацію у кожній країні та під особливості продукту відбуватимуться коригування та розробники стикатимуться з перепонами та протиріччями. Але слід розуміти, що ініціативі урядів, спрямовані на захист даних громадян, а у більш широкому розумінні – їхньої безпеки (помилково вважати, що цифрова та фізична безпека є відокремленими), мають у першу чергу підтримуватися саме розробниками та надавачами послуг, які повинні з самого початку дотримуватися високих стандартів – і стосовно технічної складової, і репутаційної. Відзначимо, що застосування законів про захист даних у різних державах-членах є неоднаковим, що ускладнює транскордонну діяльність.

Загальний регламент про захист даних (GDPR) – General Data Protection Regulation, Регламент ЄС 2016/679 – це закон ЄС, що визначає політики у сфері конфіденційності та безпеки даних. Він був офіційно прийнятий 27.04.2016 р. та набув чинності у всіх державах-членах ЄС з 25.05.2018 р. [11] Національні органи з захисту даних (DPA) висловили занепокоєння щодо права громадян на конфіденційність в Інтернеті [3]. Як виявилося на практиці, одного цього документу виявилося недостатньо, так як стрімкий розвиток цифрових послуг та бізнес-моделей на їх основі постійно вимагав уточнень та роз'яснень специфічної термінології, а деякі випадки взагалі не мали прецедентів. Тому через декілька років GDPR був доповнений так званими законами-супутниками, які уточнювали спірні положення й розширювали ті напрямки, які не були достатньо роз'яснені. Зрозуміло, що у галузі цифрових технологій значні зміни можуть відбутися і за рік, тому стан ринку онлайн послуг у 2018 р. відрізняється від того, який був у 2022–2025 рр., коли законодавство ЄС, що регулює цифрову сферу, набуло подальшого розширення, та й нечесні надавачі послуг знайшли шляхи обходження вимог, які потрібно було перекрити (ключовими роками були 2022–2023 – саме тоді розроблявся текст суміжних нормативних документів).

Основні права користувача відповідно до GDPR такі: (1) право на доступ – фізичні особи можуть вимагати доступу до своїх персональних даних і розуміти, як вони використовуються; (2) право на виправлення – користувачі можуть виправляти неточні або неповні дані; (3) право на видалення («право бути забутим») – користувачі мають право вимагати видалення своїх даних, коли вони більше не потрібні або обробляються незаконно; (4) право на перенесення даних – користувачі можуть передавати свої дані між постачальниками послуг; (5) право на заперечення проти обробки даних, особливо для прямого маркетингу; (6) право на інформування – прозорість щодо збору та використання даних є обов'язковою; (7) право на обмеження обробки – фізичні особи можуть обмежувати використання своїх даних у певних випадках. Про порушення безпеки даних надавач повинен повідоми наглядові органи (а також постраждалих осіб, якщо порушення здатне спричинити для них високий ризик) протягом 72 годин. За серйозні порушення можуть бути накладені штрафи в розмірі до 20 мільйонів євро або 4% від сукупного річного обороту.

Перейдемо до нормативних документів-супутників, які додають та закріплюють засади GDPR.

Закон про цифрові послуги (DSA), офіційно відомий як Регламент ЄС 2022/2065, є знаковим документом, прийнятою ЄС для регулювання цифрових послуг та платформ. Він набрав чинності 17.02.2024 р. і застосовується до всіх посередницьких послуг, що надаються в ЄС, незалежно від того, чи базуються постачальники та/або інфраструктура в ЄС чи за його межами [12]. DSA доповнює Закон про цифрові ринки (DMA), разом утворюючи два основоположні елементи цифрового регулювання ЄС. Цілі та сфера застосування DSA можна описати такими напрямами: (1) забезпечення безпечнішого цифрового середовища для користувачів; (2) захист основних прав користувачів в Інтернеті; (3) підвищення прозорості та підзвітності онлайн-платформ; (4) сприяння інноваціям та конкурентоспроможності, особливо для малих

та середніх підприємств (МСП) та стартапів. Він застосовується до широкого спектру цифрових послуг, зокрема соціальних мереж, онлайн точок продажу, магазинів застосунків, хмарних хостингових послуг, провайдерів інтернет-доступу, реєстраторів доменних імен, VPN та мереж доставки контенту. Пріоритетами Закону є: (1) модерація контенту та виключення (шляхом прямої заборони чи запобіжних заходів) незаконного контенту; (2) прозорість та підзвітність – платформи повинні публікувати щорічні звіти, а дуже великі онлайн-платформи (VLOP – very large online platforms) та пошукові системи (VLOSE – very large online search engines) із понад 45 мільйонами користувачів на місяць мають ще суворіші зобов'язання, включаючи оцінку ризиків і незалежний аудит; (3) прозорість реклами та алгоритмів; (4) доступ до даних для дослідників – особливо з метою перевірки на наявність дезінформація та мова ворожнечі; (5) захист неповнолітніх шляхом налаштування конфіденційності та посиленим вимогам до контенту.

Якщо згрупувати цифрові послуги за типом, то узагальнити встановлені DSA вимоги до надавачів можна за такими категоріями: посередницькі послуги – механізми повідомлення та реагування на незаконний контент; хостингові послуги – видаляти незаконний контент та надавати звіти про прозорість; онлайн-платформи – внутрішні механізми подання скарг та пояснювати рішення щодо модерації; VLOP/VLOSE –заходи щодо зменшення ризиків, незалежний аудит та підвищена прозорість. Забезпечення дотримання вимог Закону покладається на національні регуляторні органи та Європейську комісію. Недотримання вимог може призвести до штрафів у розмірі до 6% від консолідованого річного обороту. Комісія вже розпочала розслідування щодо таких платформ, як X (раніше Twitter) та TikTok, за підозрою в порушеннях, пов'язаних з модерацією контенту та прозорістю.

Закон про цифрові ринки (DMA) – Регламент ЄС 2022/1925 – був запроваджений для забезпечення справедливих і конкурентних цифрових ринків. Він набрав чинності 01.11.2022 р. і став застосовуватися з 02.05.2023 р. [14]. DMA спрямований на демонополізацію впливу на ринку великих технологічних гравців шляхом регулювання діяльності компаній, визначених як «воротарі» («гейткіпери», від англ. "gatekeepers"), тобто тих, що контролюють доступ до основних цифрових послуг. Це необхідно, адже великі цифрові платформи лише частково керуються стратегічною антиконкурентною поведінкою або антиконкурентним законодавством про злиття [2]. Основні цілі DMA: (1) сприяти справедливій конкуренції на цифрових ринках; (2) запобігати зловживанню домінуючим становищем великими платформами; (3) сприяти інноваціям та надавати можливість вибору споживачам; (4) забезпечити сумісність та прозорість цифрових послуг. Закон визначив ряд термінів, які прямо чи опосередковано сприяють найбільш наближеній до реальних практичних умов класифікації ключових гравців ринку:

«гейткіпери»/»воротарі» – це великі цифрові платформи, які надають основні платформні послуги (core platform services – CPS), такі як пошукові системи, магазини застосунків, соціальні мережі, хмарні послуги та рекламні платформи. Вони мають значний вплив на внутрішній ринок та виступають важливими посередниками (пунктами пропуску) для бізнес-користувачів на їхньому шляху до споживачів. Як правило, такі платформи займають міцну і стійку позицію на ринку. Прикладами є Alphabet (Google), Apple, Meta (Facebook), Amazon, Microsoft і ByteDance (TikTok). Основні платформні послуги (CPS) включають: інтернет-пошукові системи, соціальні мережі, платформи для обміну відео, операційні системи, веб-браузери, віртуальні помічники, маркетплейси (від англ. marketplaces – площадки-агрегатори електронної торгівлі) та рекламні послуги.

Велику увагу Закон приділяє діяльності гейткіперів, на яких прямо покладаються певні зобов'язання та заборони (табл.). Недотримання вимог може призвести до штрафів у розмірі до 10% від консолідованого річного обороту (20% за повторні порушення). Гейткіпери зобов'язані: дозволяти користувачам видаляти попередньо встановлені застосунки; забезпечувати сумісність між службами обміну повідомленнями; отримувати явну згоду на об'єднання даних між сервісами; забезпечувати справедливий доступ до магазинів застосунків та операційних систем; інформувати Європейську комісію про злиття та поглинання; подавати звіти про дотримання вимог та проходити незалежні аудити. Їм заборонено: надавати перевагу власним продуктам або послугам; перешкоджати користувачам змінювати сервіси або провайдерів; повторно використовувати персональні дані між сервісами без згоди користувачів; обмежувати доступ третіх сторін до основних функцій платформи.

Єдиним органом, що забезпечує дотримання DMA, є Європейська комісія, тоді як спільна команда DG COMP та DG CONNECT здійснює нагляд за впровадженням його вимог. Останні є генеральними директоратами в складі Європейської комісії, кожен з яких має окремі повноваження у сфері цифрової політики та конкуренції. Генеральний директорат з питань конкуренції DG COMP (Directorate-General for Competition) зосереджується на конкурентному праві, зокрема на таких питаннях, як моніторинг діяльності картелів,

злиттів та поглинань і наданні державних дотацій. Генеральний директорат з питань комунікаційних мереж, контенту та технологій DG CONNECT (Directorate-General for Communications Networks, Content and Technology) відповідає за цифрову політику, зокрема за цифрову інфраструктуру, зв'язок та єдиний цифровий ринок.

Закон про управління даними (DGA) – Регламент ЄС 2022/868 – є основою більш широкої стратегії ЄС у сфері даних, яка має на меті створити єдиний ринок даних, що сприятиме інноваціям, економічному зростанню та суспільній користі. DGA набрав чинності 23.06.2022 р. і став застосовуватися з 24.09.2023 р. [14]. Завдання DGA: (1) сприяти надійному обміну даними між різними секторами діяльності, галузями та країнами; (2) сприяти повторному використанню захищених даних державного сектору; (3) забезпечити прозору та безпечну роботу посередницьких послуг у сфері даних; (4) заохочувати альтруїзм у сфері даних – добровільний обмін даними для загального добробуту. Закон містить специфічну термінологію відповідно до специфічних об'єктів регулювання, ключовими компонентами якої є: повторне використання захищених даних державного сектору; послуги посередництва у сфері даних; альтруїзм у сфері даних; створення нового консультативного органу – Європейської ради з інновацій у сфері даних (EDIB – European Data Innovation Board), до складу якої входять національні органи влади та експерти. DGA застосовується як до персональних, так і до неперсональних даних, і діє разом із GDPR у сфері захисту персональних даних. Закон має екстериторіальну дію: організації, що не є членами ЄС, але надають послуги в ЄС, повинні призначити юридичного представника в одній з країн-членів ЄС. DGA зобов'язує виконувати правові та технічні заходи безпеки. Органи державного сектору повинні впровадити технічні заходи, такі як псевдонімізація та безпечні середовища доступу. Послуги посередництва в обміні даними повинні забезпечувати переносимість даних, прозорість та контроль користувачів. Організації, що займаються альтруїстичним використанням даних, повинні забезпечити чіткі механізми надання згоди та можливість відкликання згоди в будь-який час.

Закон про дані (Регламент ЄС 2023/2854) є знаковим нормативно-правовим актом, прийнятим в рамках Європейської стратегії у сфері даних. Він має на меті розкрити потенціал даних, що генеруються підключеними пристроями та послугами, забезпечивши справедливий доступ до них та їх використання в цифровій економіці ЄС. Закон набрав чинності в січні 2024 р. і вступає у дію 12.09.2025 р. [15]. Мета Закону полягає у наступному: (1) надати користувачам (фізичним особам та підприємствам) можливість отримувати доступ до даних, які вони генерують, та контролювати їх; (2) сприяти справедливості в обміні даними, особливо між великими та малими учасниками ринку; (3) спростити перехід між хмарними та периферійними послугами; (4) забезпечити доступ державного сектору до приватних даних у надзвичайних ситуаціях; (5) захистити від несправедливих договірних умов в угодах про обмін даними.

Основні терміни та процеси, які підпадають під його дію:

1. Доступ до даних з підключених пристроїв. Користувачі підключених продуктів (наприклад, розумних холодильників, промислових машин, медичних пристроїв) мають право на доступ до даних, які вони генерують. Виробники повинні зробити ці дані легко доступними, за винятком випадків, коли вони є високозбагаченими або отриманими за допомогою запатентованих алгоритмів. Це стосується як сирих, так і попередньо оброблених даних, але не описових або високозбагачених даних.

2. Обов'язки щодо обміну даними. Користувачі можуть обмінюватися своїми даними з третіми сторонами на свій вибір. Власники даних (наприклад, виробники) повинні сприяти такому обміну без накладення несправедливих умов. Ця норма включає положення щодо доступу наступних користувачів (наприклад, власників вживаних пристроїв) до історичних даних із забезпеченням захисту конфіденційності та комерційної таємниці.

3. Справедливі договірні умови. Захищає підприємства, особливо МСП, від несправедливих положень у договорах про обмін даним; впроваджує рамки для переговорів про справедливі умови, з типовими положеннями та механізмами вирішення спорів.

4. Перехід між хмарними та периферійними послугами – встановлюються мінімальні вимоги до взаємодії хмарних та периферійних послуг. Користувачі повинні мати можливість змінювати постачальників без надмірного навантаження, витрат або перебоїв у роботі. Ця норма вирішує проблему залежності від постачальника та сприяє конкуренції на ринку обробки даних.

5. Доступ державного сектору в надзвичайних ситуаціях – норма дозволяє державним органам вимагати доступ до приватних даних під час надзвичайних ситуацій (наприклад, повеней, лісових пожеж та інших стихійних лих). Доступ повинен бути пропорційним, обмеженим у часі та підлягати гарантіям.

Закон про дані застосовується до даних, створених в ЄС, незалежно від місцезнаходження власника даних, і поширюється на персональні та неперсональні дані, доповнюючи GDPR щодо персональних даних; що важливо,

застосовується до готових підключених продуктів, що розміщуються на ринку ЄС, а не до прототипів. Встановлюються такі запобіжні заходи та обмеження: (1) торгові таємниці та інтелектуальна власність захищаються за допомогою технічних та правових запобіжних заходів; (2) обмін даними повинен відбуватися з повагою до права на приватність, з чіткими межами щодо того, до яких даних можна отримати доступ або які дані можна обмінювати; (3) технології підвищення рівня конфіденційності (PETs – Privacy-enhancing technologies) заохочуються, але не звільняють від обов'язку обміну даними.

Закон про дані є так званим «горизонтальним регулюванням» – він застосовується в усіх секторах і доповнює інші закони ЄС у галузі охорони та управління даними, а саме: GDPR (захист персональних даних), DGA (довіра та альтруїзм у обміні даними), DMA (конкуренція платформ), Закон про штучний інтелект та Закон про кіберстійкість (управління новими технологіями).

Отже, зростаюча кількість нормативних вимог ЄС у останні роки змінила процедури закупівлі, вимоги до зберігання даних, безпеки та взаємодії. Низці вимог тепер повинні відповідати й імпортовані хмарні та SaaS-інструменти для розробників. Якоюсь мірою це може стосуватись і т.зв. «супердодатків» (super-apps), у сфері злиття та поглинання, партнерств та інших стратегічних альянсів, які відіграють вирішальну роль у розвитку крупних IT-компаній [6], а також стратегію цифрових фінансів, метою якої є зробити фінансові послуги більш дружніми до цифрових технологій і стимулювати відповідальні інновації та конкуренцію серед постачальників [7]. Цифрові технології розглядаються як важлива передумова руху до сталого розвитку [8]. Зведені вимоги основних нормативних документів, що регулюють сферу управління даними, наведено у табл. 1 [5, 9, 11–15]:

Таблиця 1

Ключові нормативні документи ЄС у сфері управління даними

Сфера регулювання	Принципові вимоги	Вплив на постачальників послуг
Закон про цифрові послуги – Digital Services Act (DSA)		
Застосовується до всіх посередницьких послуг (включаючи хостинг коду, реєстри пакетів, платформи CI/CD) з користувачами з ЄС	• Терміни видалення незаконного контенту та прозорість звітності • Управління ризиками для системних платформ (50 млн+ користувачів в ЄС)	• Необхідність призначати законного представника в ЄС • Щоквартальні аудити відповідності незалежними оцінювачами • Більш суворі процеси модерації та відшкодування збитків користувачам
Закон про цифрові ринки – Digital Markets Act (DMA)		
Націлений на «воротарів» з сильною залежністю від інфраструктури системи (наприклад, великі постачальники хмарних послуг або репозиторіїв)	• API для взаємодії між системами для обміну повідомленнями та експорту даних • Відсутність самопреференцій для внутрішніх інструментів • Забезпечення механізму перенесення даних розробників та робочих процесів	• Менший ризик прив'язки до постачальника для європейських команд • Обов'язкова відкритість великих іноземних платформ, що працюють в ЄС
Загальний регламент про захист даних – General Data Protection Regulation (GDPR)		
Передача даних: постачальники з третіх країн повинні покладатися на механізми, затверджені ЄС, утому числі на стандартні договірні умови (Standard Contractual Clauses –SCC) та рішення про адекватність	• Явна згода або законний інтерес щодо метаданих розробників (журнали, використання) • Оцінка впливу на захист даних для обробки з високим ризиком	• Міграція даних, пов'язаних з користувачами та проектами, до центрів обробки даних, розташованих в ЄС • Більша складність контрактів (стандартні договірні умови, ст. 28 про обробників даних)
Закон про управління даними та Закон про дані – Data Governance Act & Data Act		
Заохочує створення галузевих інфраструктур для обміну даними (наприклад, у сфері промислового виробництва, охорони здоров'я)	Повторне використання публічних даних: державні органи повинні надавати API на справедливих, недискримінаційних умовах	• Імпортовані аналітичні або ML-сервіси потребують прозорих ліцензій на обмін даними • Простіший доступ до публічних наборів даних ЄС для європейських розробників

Існує низка ще більше деталізованих нормативних документів, основною метою яких є не тільки захист даних користувачів, а й роз'яснення щодо технологічних процедур та окремих рішень.

NIS2 (Директива ЄС 2022/2555) є оновленим нормативним документом в галузі кібербезпеки [16]. Вона замінює Директиву NIS (2016/1148) і має на меті встановити високий загальний рівень кібербезпеки в усьому ЄС. Прийнята 14.12.2022 р., повне впровадження розпочалося 18.10.2024 р. NIS2 є частиною більш широкої цифрової стратегії ЄС і доповнює інші ініціативи, такі як Закон про кіберстійкість, Закон про цифрову операційну стійкість (DORA – Digital Operational Resilience Act) та Закон ЄС про кібербезпеку. NIS2 має на меті: посилити кібербезпеку в критично важливих секторах; поліпшити процедуру реагування на інциденти та управління ризиками; посилити співпрацю у межах ЄС; забезпечити підзвітність та нагляд за управлінням кібербезпекою.

Окрім іншого, відповідно до NIS2 органи влади можуть проводити аудити, накладати штрафи та забезпечувати дотримання вимог у галузі цифрового законодавства. Штрафи можуть включати адміністративні штрафи та тимчасові заборони на діяльність. Директива зазначає, що взаємні перевірки між державами-членами сприяють узгодженій діяльності та співпраці у сфері цифрової економіки. Галузі, на які поширюється дія NIS2, включає різних галузевих суб'єктів ринку та розподіляє їх на групи за ступенем критичності дотримання вимог.

Основні суб'єкти – це підприємства таких галузей, як енергетика (електроенергія, нафта, газ), транспорт (повітряний, залізничний, водний, автомобільний), банки та фінансові установи, заклади охорони здоров'я, підприємства, що займаються транспортуванням та очищенням питної води та стічних вод, цифрова інфраструктура (DNS, хмарні технології, центри обробки даних).

Важливі суб'єкти – це підприємства, які забезпечують поштові та кур'єрські послуги, управління відходами, відносяться до хімічної та харчової промисловості, виробництва (фармацевтика, електроніка, транспортні засоби), а також дослідницькі організації та цифрові провайдери (торгові онлайн-площадки, пошукові системи, соціальні медіа).

Відповідно підприємствам необхідно інтегрувати вимоги щодо кібербезпеки в основні операції, дотримуватися більш суворих вимог щодо дотримання норм та звітності, запровадити проактивне управління ризиками, пов'язаними з третіми сторонами та ланцюгами постачання.

Закон про кіберстійкість (CRA) був прийнятий 10.12.2024 р., повні зобов'язання за яким набирають чинності з 11.12.2027 р. [17]. Це перший у світі законодавчий акт, що встановлює комплексні вимоги до кібербезпеки продуктів з цифровими елементами (PDEs – products with digital elements), включаючи як апаратне, так і програмне забезпечення, протягом усього їхнього життєвого циклу. CRA є частиною більш широкої стратегії ЄС у сфері цифрової та кібербезпеки, доповнюючи Директиву NIS2, Закон про цифрову операційну стійкість (DORA) та Закон ЄС про кібербезпеку. Головні завдання CRA: (1) високий рівень кібербезпеки цифрових продуктів, що продаються в країнах ЄС; (2) сприяння принципам безпеки за замовчуванням та безпеки за замовленням; (3) покращення прозорості для споживачів та підприємств; (4) зменшення фрагментації та правової невизначеності в державах-членах ЄС.

Закон застосовується до всіх продуктів з цифровими елементами, які прямо або опосередковано підключаються до пристрою або мережі: розумні пристрої (наприклад, дитячі монітори, розумні телевізори, іграшки); промислові системи управління; операційні системи, вбудоване програмне забезпечення, бібліотеки; брандмауери, маршрутизатори та компоненти Інтернету речей. Виключенням з переліку є продукти, які вже регулюються іншими законами ЄС, такі як: медичні вироби, автомобільні транспортні засоби, авіаційні системи та некомерційне програмне забезпечення з відкритим кодом (хоча комерційні продукти, що використовують компоненти з відкритим кодом, підпадають під дію Закону). Дія Закону поширюється на всі продукти, що розміщуються на ринку ЄС, незалежно від країни походження – як до виробників та дистриб'юторів з ЄС, так і до виробників та дистриб'юторів з країн, що не входять до ЄС. Принципові вимоги, які значно підсилюють відповідальність розробників та надавачів цифрових послуг стосовно безпеки продукту, такі: (1) безпека за замовчуванням – кібербезпека повинна бути інтегрована на найраніших етапах розробки продукту, а продукти повинні мати безпечні конфігурації за замовчуванням і уникати небезпечних опцій; (2) безпека протягом життєвого циклу – виробники несуть відповідальність протягом усього життєвого циклу продукту, включаючи своєчасні оновлення безпеки, управління патчами та розкриття вразливостей; (3) прозорість – продукти повинні містити чіткі повідомлення про наявні функції кібербезпеки, щоб користувачі мали можливість робити обґрунтований вибір.

Забезпечення дотримання вимог Закону покладається на національні органи влади, які здійснюватимуть моніторинг та проводитимуть аудити. Недотримання вимог може призвести до вилучення продукції з ринку, накладання

штрафів та санкцій, публічного розкриття вразливостей. Введення у дію Закону зобов'язує виробників переглянути процеси розробки продукції з метою інтеграції кібербезпеки та понести нові витрати на дотримання вимог та сертифікацію. У свою чергу, споживачі матимуть впевненість у безпеці продукції з маркуванням CE і отримуватимуть прозоріші цифрові пристрої.

Нормативно-правова база в галузі штучного інтелекту, як стверджують автори [4], наразі складається з п'яти категорій: 1) регулювання штучного інтелекту, 2) обробка даних, 3) оцінка технологій, 4) підтримка інновацій та 5) охорона здоров'я та права людини. Основним є Закон ЄС про штучний інтелект (Регламент ЄС 2024/1689) – перший в світі комплексне правове джерело для регулювання штучного інтелекту. Він був прийнятий у травні 2024 року, опублікований в Офіційному віснику ЄС 12.07.2024 р. і набрав чинності 01.08.2024 р. [18]. Його положення будуть впроваджуватися поетапно протягом 2025–2027 років, а повне застосування очікується до 2030 року (тому у деяких джерелах він має назву Проекту закону).

Закон застосовується до всіх систем ШІ, що використовуються в ЄС, незалежно від місця їх розробки або впровадження, і поширюється на розробників, розгортачів та користувачів систем ШІ. Він включає моделі ШІ загального призначення (GPAI – general purpose artificial intelligence), такі як великі мовні моделі (LLM – large language models), та системи ШІ з високим рівнем ризику, що використовуються в чутливих сферах. Закон запроваджує багаторівневу систему дотримання вимог, засновану на рівні ризику, який становлять системи ШІ: неприйнятний рівень ризику – категорично заборонено (наприклад, соціальний рейтинг, маніпулятивний ШІ, використання вразливостей); високий – суворі зобов'язання (біометрична ідентифікація, кредитний рейтинг, медичні пристрої, інструменти для підбору персоналу); обмежений – вимоги щодо прозорості (чат-боти, дипфейки повинні повідомляти про використання ШІ); мінімальний – немає конкретних зобов'язань (наприклад, спам-фільтри, ШІ у відеоіграх).

Зобов'язання відповідно до категорії продукції наступні (табл. 2) [18]:

Контроль за дотриманням Закону здійснюється новоствореним Управлінням ЄС з питань ШІ (EU AI Office) та національними органами влади. Штраф за недотримання вимог встановлений у розмірі до 35 млн євро або 7% від консолідованого річного обороту, залежно від того, яка сума є більшою, і включає заборону на продаж продукції, яка порушує вимоги, її відкликання та публічні повідомлення про серйозні порушення.

У липні 2025 року було опубліковано добровільний, але впливовий Кодекс практик для систем ШІ загального призначення (Code of Practice for GPAI). Він охоплює найкращі практики щодо прозорості, безпеки та дотримання авторських прав, і був підписаний такими великими постачальниками, як OpenAI, Google та Anthropic; Meta відмовилася підписати, посилаючись на занепокоєння щодо надмірного втручання.

Як наслідок, підприємствам необхідно оцінювати та класифікувати системи ШІ, впровадити системи управління та механізми дотримання вимог, працювати в умовах підвищених юридичних та репутаційних ризиків. Заплановано такий графік впровадження: лютий 2025 р. – заборонені системи заблоковані; починають діяти загальні положення; серпень 2025 р. – починають діяти зобов'язання щодо GPAI; активовано систему штрафних санкцій; серпень 2026 р. – застосовуються зобов'язання щодо ШІ з високим рівнем ризику (наприклад, у сферах охорони здоров'я, управління персоналом, кредитування); серпень 2027–2030 рр. – прийняття галузевих правил та забезпечення відповідності існуючих систем.

У табл. 3 узагальнено ключові вимоги зазначених вище нормативних документів стосовно цифрового продукту [10, 16–19].

Що стосується сплати ПДВ, то станом на серпень 2025 р. існують наступні вимоги. Будь-яке підприємство (що має юридичну адресу у ЄС або поза ЄС), яке продає цифрові послуги приватним

Таблиця 2

Вимоги до продукції із компонентою ШІ за категоріями

Вид продукту	Вимоги до розробників / надавачів
Системи ШІ з високим рівнем ризику	– проводити оцінку ризиків та перевірку відповідності; – вести технічну документацію та реєстрацію; – забезпечувати людський нагляд, точність та надійність; – реєструвати системи в базі даних ШІ ЄС; – повідомляти органи влади про серйозні інциденти або несправності.
Моделі ШІ загального призначення (GPAI)	– надавати технічну документацію та резюме навчальних даних; – дотримуватися законодавства ЄС про авторське право; – проводити перехресні випробування та оцінку системних ризиків; – забезпечити заходи з кібербезпеки та розкриття інформації про енергоефективність.

Таблиця 3

Нормативні документи ЄС у галузі цифрових послуг

Сфера регулювання	Принципові вимоги	Вплив на постачальників послуг
Директива про мережеві та інформаційні системи та Закон про кіберстійкість – Network and Information Systems (NIS2) Directive 2022/2555 & Cyber Resilience Act		
Розширює зобов'язання з кібербезпеки на більшу кількість постачальників цифрових послуг, включаючи хмарні та хостингові послуги	Впроваджуються вимоги щодо безпеки на етапі проектування для апаратних та програмних засобів	• Обов'язкове повідомлення про інциденти протягом 24 годин • Регулярні оновлення безпеки та розкриття вразливостей
Закон про штучний інтелект – AI Act (Artificial Intelligence Act)		
Послуги штучного інтелекту класифікуються за рівнем ризику від мінімального до неприйнятного	• Оцінка відповідності для штучного інтелекту з високим ризиком (наприклад, генерація коду, засоби автоматизованого тестування) • Зобов'язання щодо прозорості (обов'язок вказувати, що «цей результат був згенерований штучним інтелектом»)	• Імпортовані API штучного інтелекту повинні надавати документацію щодо даних для навчання, зменшення упередженості та продуктивності
Політика стосовно ПДВ та оподаткування цифрових послуг (окремого документу немає, вимоги містяться у профільних документах)		
Єдине вікно (One-Stop Shop – OSS): спрощує дотримання вимог щодо ПДВ для транскордонних цифрових поставок B2B та B2C	Правила місця постачання: цифрові послуги оподатковуються за місцем реєстрації клієнта	• Постачальники повинні зареєструватися в «єдиному вікні» (OSS) • Автоматичне формування рахунків-фактур відповідно до режиму ПДВ, що діє в ЄС

споживачам в ЄС, підпадає під зазначені нижче регулювання. До переліку надаваних послуг входять: програмне забезпечення, застосунки, потокове передавання, електронні книги, онлайн-курси та інші послуги, що надаються в електронному вигляді.

З 2015 року ПДВ повинен стягуватися за місцезнаходженням споживача, а не продавця. Тому підприємства-експортери повинні застосовувати місцеву ставку ПДВ країни ЄС, в якій проживає їхній клієнт. Якщо річний обсяг продажів цифрових товарів та послуг резидентам ЄС не перевищує 10 000 євро, можна застосовувати правила ПДВ своєї країни. Якщо ж обсяг продажів перевищує цю суму, підприємець повинен зареєструватися в OSS і сплачувати ПДВ відповідно до місцезнаходження клієнта.

Існують спеціальні правила оподаткування ПДВ, що стосуються українських компаній, які експортують цифрові послуги до ЄС, зокрема відповідно до правил ЄС щодо місця постачання та власної системи оподаткування ПДВ в Україні, але в основному застосовуються загальні правила та рекомендації.

Місце постачання визначає обов'язок сплати ПДВ – для B2C цифрових послуг (наприклад, потокового передавання, хмарних послуг, завантаження програмного забезпечення) місцем постачання є місцезнаходження клієнта. Українські компанії повинні стягувати ПДВ за ставкою, що застосовується в країні ЄС, де знаходиться клієнт. Для спрощення дотримання вимог підприємства, що не є членами ЄС, можуть скористатися схемою єдиного вікна (OSS): 1) зареєструватися в одній країні ЄС; 2) подавати одну квартальну декларацію з ПДВ, що охоплює всі продажі в ЄС. Таким чином, централізовано сплачене ПДВ потім розподіляється між відповідними державами-членами. Цифрові послуги, на які поширюється дія відповідних норм, включають: доступ до програмного забезпечення, ігор, музики, відео або їх завантаження; хмарні обчислювальні послуги; інтернет-реклама; платформи контенту на основі передплати.

Компанії-нерезиденти, які надають цифрові послуги фізичним особам в Україні, повинні зареєструватися платниками ПДВ в Україні, якщо їх річний дохід перевищує 1 мільйон гривень (~32 000 євро). Ставка ПДВ становить 20%, реєстрація та звітність здійснюються через спеціальний онлайн-портал.

B2B або цифрові послуги, що експортуються з України до підприємств ЄС (B2B), як правило, звільнені від українського ПДВ, оскільки місце постачання знаходиться за межами України.

Українські компанії повинні документально підтвердити статус клієнта з ЄС (наприклад, шляхом перевірки номера ПДВ), щоб підтвердити статус B2B.

Таким чином, загальні поради для українських експортерів наступні: (1) зареєструватися в EU OSS, якщо підприємство надає цифрові послуги B2C у декількох країнах ЄС; (2) вести чітку документацію про місцезнаходження клієнтів та їхній статус платника ПДВ; (3) слідкувати за пороговими значеннями та оновленнями нормативно-правових актів, особливо в міру того, як Україна наближається до податкових норм ЄС.

Висновки з проведеного дослідження. Ринок цифрових послуг у країнах ЄС, зважаючи на високу платоспроможність користувачів та різноманітність задач, є надзвичайно привабливим для українських розробників. Проте, необхідно зважати на останні зміни у законодавстві, які спрямовані не тільки на підвищення рівня безпеки управління даними користувачів, а й подекуди висувають вимоги технічного характеру, що потребує від розробників включення додаткового функціоналу до продукту чи інтеграцію певних протоколів та виконання процедур, які можуть бути необов'язковими в Україні чи інших зарубіжних ринках. У сфері податкового регулювання, зокрема сплати ПДВ, запроваджені незвичні для більшості національних компаній підходи, як-от механізм зворотного зарахування. Навіть якщо українське підприємство, надаючи послуги користувачу з ЄС у сегменті B2B, не повинне самостійно сплачувати ПДВ, варто попереджати про особливості такого механізму покупця, особливо якщо він користувався до цього послугами виключно внутрішніх розробників.

Список використаних джерел:

1. Eurostat. URL: https://ec.europa.eu/eurostat/data/statistical-themes
2. Fletcher A., Cremer J., Heidhues P. et al. The effective use of economics in the EU Digital Markets Act. *Journal of Competition Law & Economics.* 2024. № 20. Pp. 1–19. DOI: https://doi.org/10.1093/joclec/nhad018
3. Heidebrecht S. From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. *Journal of Common Market Studies.* 2024. Volume 62. Number 1. Pp. 205–223. DOI: https://doi.org/10.1111/jcms.13488
4. Schmidt J., Schutte N.M., Buttigieg S. et al. Mapping the regulatory landscape for artificial intelligence in health within the European Union. *npj Digital Medicine.* 2024. № 7. Art. 229. DOI: https://doi.org/10.1038/s41746-024-01221-6
5. Sharon T., Gellert R. Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. *Information, Communication & Society.* 2023. № 27(15). Pp. 2651–2668. DOI: https://doi.org/10.1080/1369118X.2023.2246526
6. van der Vlist F. N., Helmond A., Dieter M., Weltevrede E. Super-appification: Conglomeration in the global digital economy. *New Media & Society.* 2024. № 27(6). Pp. 3314–3337. DOI: https://doi.org/10.1177/14614448231223419
7. Васильчук І.П., Слюсаренко К.В. Цифрова фінансова стратегія ЄС: виклики та можливості для України. *Інженерні інновації та розбудова національної економіки* : матеріали І Міжнародної науково-практичної конференції Інженерного навчально-наукового інституту ім. Ю. М. Потебні (09–10 травня 2024 року, м. Запоріжжя) / наук. ред. Н. Г. Метеленко ; Інженерний навчально-науковий інститут ім. Ю. М. Потебні Запорізького національного університету. Одеса, «Гельветика», 2024. 1020 с. С. 301–305. URL: https://www.znu.edu.ua/ii_znu/nauka/conf10/zbirnyk_24.pdf
8. Іванцов С. Стратегічні орієнтири розвитку цифрової економіки у ЄС. *Modeling the Development of the Economic Systems.* 2024. № 4. С. 186–192. DOI: https://doi.org/10.31891/mdes/2024-14-25
9. Ковбас І. В., Редько О. М. Електронне урядування в країнах Європейського Союзу та в Україні. *Академічні візії.* 2025. № 41. URL: https://www.academy-vision.org/index.php/av/article/view/1836
10. Шворак Л.О., Гуменюк Я.О. Ринок цифрових послуг в центрі регуляторної політики ЄС. *Економічний простір.* 2024. № 193. С. 138–143. URL: http://srd.pgasa.dp.ua:8080/handle/123456789/13921
11. General Data Protection Regulation (Regulation (EU) 2016/679). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
12. Digital Services Act (Regulation (EU) 2022/2065). URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj
13. Digital Markets Act (Regulation (EU) 2022/1925). URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj
14. Data Governance Act (Regulation (EU) 2022/868). URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj
15. Data Act (Regulation (EU) 2023/2854). URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj
16. NIS 2 (Directive (EU) 2022/2555). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
17. Cyber Resilience Act (Regulation (EU) 2024/2847). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj
18. Artificial Intelligence Act (Regulation (EU) 2024/1689). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
19. Consumption taxes, DOI OECD. URL: https://www.oecd.org/tax/consumption/international-vat-gst-guidelines.htm

References:

1. Eurostat. Available at: https://ec.europa.eu/eurostat/data/statistical-themes
2. Fletcher A., Cremer J., Heidhues P. et al. (2024). The effective use of economics in the EU Digital Markets Act. *Journal of Competition Law & Economics,* vol 20, pp. 1–19. DOI: https://doi.org/10.1093/joclec/nhad018
3. Heidebrecht S. (2024). From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. *Journal of Common Market Studies,* vol. 62, No 1, pp. 205–223. DOI: https://doi.org/10.1111/jcms.13488
4. Schmidt J., Schutte N.M., Buttigieg S. et al. (2024). Mapping the regulatory landscape for artificial intelligence in health within the European Union. *npj Digital Medicine,* vol. 7, art. 229. DOI: https://doi.org/10.1038/s41746-024-01221-6
5. Sharon T., Gellert R. (2023). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. *Information, Communication & Society,* vol. 27(15), pp. 2651–2668. DOI: https://doi.org/10.1080/1369118X.2023.2246526
6. van der Vlist F. N., Helmond A., Dieter M., Weltevrede E. (2024). Super-appification: Conglomeration in the global digital economy. *New Media & Society,* vol 27(6), pp. 3314–3337. DOI: https://doi.org/10.1177/14614448231223419
7. Vasylchuk I.P., Sliusarenko K.V. (2024). Tsyfrova finansova stratehiia YeS: vyklyky ta mozhlyvosti dlia Ukrainy [The EU's digital financial strategy: challenges and opportunities for Ukraine]. *Inzhenerni innovatsii ta rozbudova natsionalnoi ekonomiky* : materialy I Mizhnarodnoi naukovo-praktychnoi konferentsii Inzhenerno-ho navchalno-naukovoho instytutu im. Yu. M. Potebni (09–10 May 2024, m. Zaporizhzhia) / nauk. red. N. H. Metelenko ; Inzhenernyi navchalno-naukovyi instytut im. Yu. M. Potebni Zaporizkoho natsionalnoho universytetu. Odesa, "Helvetyka", 1020 p., pp. 301–305. Available at: https://www.znu.edu.ua/ii_znu/nauka/conf10/zbirnyk_24.pdf
8. Ivantsov S. (2024). Stratehichni oriientyry rozvytku tsyfrovoi ekonomiky u YeS [Strategic guidelines for the development of the digital economy in the EU]. *Modeling the Development of the Economic Systems,* vol 4, pp. 186–192. DOI: https://doi.org/10.31891/mdes/2024-14-25
9. Kovbas I. V., Redko O. M. (2025). Elektronne uriaduvannia v krainakh Yevropeiskoho Soiuzu ta v Ukraini [E-government in European Union countries and Ukraine]. *Akademichni vizii – Academic visions,* vol. 41. Available at: https://www.academy-vision.org/index.php/av/article/view/1836 (in Ukrainian)
10. Shvorak L.O., Humeniuk Y.O. (2024). Rynok tsyfrovykh posluh v tsentri rehuliatornoi polityky YeS [The digital services market at the core of EU regulatory policy]. *Ekonomichnyi prostir – Economic space,* vol 193, pp. 138–143. Available at: http://srd.pgasa.dp.ua:8080/handle/123456789/13921 in Ukrainian)
11. General Data Protection Regulation (Regulation (EU) 2016/679). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
12. Digital Markets Act (Regulation (EU) 2022/1925). Available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj
13. Digital Markets Act (Regulation (EU) 2022/1925). URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj
14. Data Governance Act (Regulation (EU) 2022/868). Available at: https://eur-lex.europa.eu/eli/reg/2022/868/oj
15. Data Act (Regulation (EU) 2023/2854). Available at: https://eur-lex.europa.eu/eli/reg/2023/2854/oj
16. NIS 2 (Directive (EU) 2022/2555). Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
17. Cyber Resilience Act (Regulation (EU) 2024/2847). Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj
18. Artificial Intelligence Act (Regulation (EU) 2024/1689). Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
19. Consumption taxes, OECD. Available at: https://www.oecd.org/tax/consumption/international-vat-gst-guidelines.htm

Стаття надійшла: 05.08.2025
Стаття прийнята: 12.09.2025
Стаття опублікована: 26.09.2025