

УДК 004:339.9(4+100)

DOI: <https://doi.org/10.30838/EP.204.68-74>**Гончаренко В.В.**

доктор економічних наук

Харківський національний університет ім. В.Н. Каразіна

**Honcharenko Vladyslav**

Dr. of Economic Sc.

V.N. Karazin Kharkiv National University

<https://orcid.org/0000-0002-0414-8892>**Пожар А.А.**

кандидат економічних наук

Полтавський університет економіки і торгівлі

**Pozhar Artem**

PhD in Economic Sc.

Poltava University of Economics and Trade

<https://orcid.org/0000-0002-8662-9074>

## ГЕОЕКОНОМІЧНІ АСПЕКТИ ЦИФРОВІЗАЦІЇ: СВІТОВИЙ РИНОК ІТ-ПОСЛУГ І СТРАТЕГІЧНІ ПРІОРИТЕТИ ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇН

*Стаття аналізує геоелекономічні засади розвитку світового ринку ІТ-послуг у контексті цифровізації та пов'язані ризики економічної безпеки держав. Мета – сформулювати цілісну рамку, що поєднує структуру ринку, режими даних і ринкову владу платформ із каналами передачі ризиків. Використано порівняльний і інституційний аналіз, методи сценарного моделювання та побудову матриці «ризик–політика». Отримано: окреслено центри впливу, ідентифіковано ключові уразливості (vendor lock-in, кіберризики, юрисдикційні обмеження даних), запропоновано інструменти контрольованої відкритості. Новизна полягає у поєднанні геоелекономічної карти центрів впливу з матрицею «ризик–політика» та сценарною валідацією консолідації/диверсифікації. Практична цінність – рекомендації для урядів і експортерів ІТ-послуг щодо збалансування відкритості й стійкості.*

**Ключові слова:** цифровізація економіки; ринок ІТ-послуг; економічна безпека; транскордонні потоки даних; хмарні сервіси; інтероперабельність; vendor lock-in; мультихмара; геоелекономіка.

## GEO-ECONOMIC DIMENSIONS OF DIGITALIZATION: GLOBAL IT SERVICES MARKET AND ECONOMIC SECURITY PRIORITIES

*The paper examines the geo-economic foundations of the global IT services market under accelerating digitalization and its implications for national economic security. The objective is to build an integrated analytical framework linking market structure, data governance regimes and platform power with the channels through which risks are transmitted. The study employs comparative and institutional analysis, scenario modelling and a risk-policy matrix across market segments. The results identify leading centres of influence and value capture, map critical vulnerabilities—vendor lock-in in cloud infrastructure, cyber-threat exposure, jurisdictional constraints on cross-border data—and demonstrate how these propagate through managed services, data/AI and platform layers. The paper proposes a policy toolbox of controlled openness: portability and interoperability of data and cloud services, multi-cloud and multisourcing strategies, certification and Zero Trust architectures, and pro-competitive remedies in cloud markets. The relevance stems from simultaneous platform consolidation and regulatory fragmentation of data flows, which reshape access to technology and value capture across borders. Methodologically, the paper triangulates policy analysis with comparative institutional mapping and case-informed assessment of switching costs in cloud markets, operationalising risks through a segment-specific matrix and scenario contrasts (consolidation, diversification, mixed). Key findings show how dependence on hyperscalers, jurisdictional data constraints and supply-chain exposures translate into systemic vulnerabilities for open and catching-up economies, and how controlled openness mitigates them without sacrificing scale or innovation. The practical value is a decision-support toolkit for governments and firms: sequencing interoperability and portability mandates, embedding Zero Trust and certification in procurement, and aligning international cooperation on cross-border data to reduce uncertainty while expanding export capacity of IT services.*

**Keywords:** digitalization of the economy; IT services market; economic security; cross-border data flows; cloud services; interoperability; vendor lock-in; multi-cloud; geoeconomics.

**JEL classification:** F02, F15, L86, O33, F23.

**Постановка проблеми.** Стрімка цифровізація перетворила ринок ІТ-послуг на ключову інфраструктуру економіки, однак його зростання супроводжується концентрацією платформ, «приватною» стандартизацією, розбіжностями режимів обігу даних і зростанням кіберризиків. Це створює асиметрії доступу до технологій і даних, посилює залежність від постачальників та ускладнює забезпечення економічної безпеки, особливо для відкритих і перехідних економік. Наявні дослідження здебільшого аналізують окремі аспекти (хмара, конкуренція, дані) ізольовано; бракує інтегрованої гео економічної рамки, яка пов'язує структуру глобального ринку, регуляторні режими та канали передачі ризиків між сегментами послуг.

**Гіпотеза дослідження.** Поєднання політик контрольованої відкритості – портованість і інтероперабельність даних/хмар, мультихмара та мультисорсинг, сертифікація і Zero Trust, а також конкурентні засоби на ринку хмар – знижує системну залежність і регуляторну невизначеність без втрати темпів інновацій та зростання, причому оптимальною траєкторією для більшості економік є «змішаний» режим між глобальними платформами та національними/регіональними вимогами.

**Аналіз останніх досліджень і публікацій.** Сучасна література розглядає цифровізацію як ключовий драйвер перерозподілу вартості у світовій торгівлі послугами та фіксує критичну роль правил даних. Gupta, Ghosh і Sridhar [4] емпірично показують, що обмеження транскордонних потоків даних статистично знижують експорт ІТ-послуг; для вимірювання «жорсткості» політик вони пропонують індекс MDRI. Паралельно Li, Han та Xu [7] доводять, що рівень цифрової зрілості економіки істотно підвищує конкурентоспроможність експорту послуг як через інтенсивну, так і екстенсивну складові. Zhang, Xu та Yang [10] на основі даних UN COMTRADE досліджують мережеву еволюцію торгівлі ІКТ-послугами (2004–2020), ідентифікуючи структурні центри впливу та зміни каналів інтеграції. На макрорівні Herman і Oliver [5] показують, що положення про цифрову торгівлю в угодах та інтернет-зв'язність підсилюють товарні й сервісні потоки та добробут, формуючи «експорт правил». Регуляторний вимір активно трансформується: Guo і Li [3] документують перехід Китаю від жорстких до більш гнучких режимів трансферу даних (у контексті PIPL/DSL/CSL), що знижує транзакційні витрати для цифрової торгівлі. На мікрорівні Shaik і Natarajan [8] пропонують інженерні рішення для зменшення vendor lock-in у хмарних БД, що напряму кореспондує з ризиками економічної безпеки, окресленими у статті.

Попри прогрес, бракує інтегрованої рамки, яка поєднала б політики даних, ринкову структуру платформ, технічні бар'єри міграції та метрики вразливості для країн-експортерів і імпортерів ІТ-послуг; цей аналітичний розрив і становить предмет нашого дослідження.

**Мета статті** – сформувати інтегровану гео економічну рамку аналізу світового ринку ІТ-послуг у контексті цифровізації та визначити стратегічні пріоритети економічної безпеки країн. Досягнення цієї мети передбачає систематизацію структури та центрів впливу ринку; виявлення каналів передачі ризиків (кіберзагрози, залежність від постачальників, юрисдикційні обмеження даних); зіставлення національних і наднаціональних режимів регулювання та моделювання сценаріїв розвитку (консолідація, диверсифікація, змішаний режим). На цій основі пропонується набір інструментів «контрольованої відкритості» – портованість та інтероперабельність даних/хмар, мультихмара і мультисорсинг, сертифікація та Zero Trust, конкурентні засоби – для мінімізації технологічних і регуляторних залежностей без втрати інноваційної динаміки.

**Виклад основних результатів дослідження.** Світовий ринок ІТ-послуг став опорною інфраструктурою цифрової економіки: саме через нього бізнес і держави масштабують інновації, керують даними та забезпечують стійкість операцій. На відміну від продажу «заліза» чи коробкового ПЗ, послуги підтримують безперервну трансформацію – від архітектури й розробки до керованої експлуатації та кіберзахисту. За оцінками СОТ, у 2023 р. експорт цифрово доставлених послуг сягнув 4,25 трлн дол. США (+9% у річному вимірі), або 13,8% світового експорту товарів і послуг; у структурі цих послуг частка комп'ютерних становила 20,5%, а сам підсектор зріс на 11% у річному вимірі [9].

Структурно ринок ІТ-послуг зазвичай поділяють на business process / application / infrastructure services з логікою design–build–run (консалтинг і архітектура → розробка та інтеграція → керовані сервіси). У практиці це проявляється конвергенцією сегментів: DevSecOps (інтеграція безпеки у всі етапи розробки та експлуатації програмного забезпечення) поєднує розробку й безпеку; «дані+AI» пронизують підтримку, інтеграцію та клієнтські сервіси; хмара переводить витрати з капітальних у операційні, прискорює time-to-market і водночас підсилює залежність від постачальників інфраструктури – технологічний фактор, що набуває гео економічного виміру.

Макророль сектору підтверджують офіційні дані: у ЄС частка ІКТ-сектору у ВДВ становила 5,5% у 2022 р. (з них ІКТ-послуги – 4,6%), причому за 2012–2022 рр. внесок ІКТ-послуг зріс на 24,8%. Паралельно зростає проникнення хмар: у 2023 р. 45% підприємств ЄС (10+ працівників) купували хмарні сервіси; у Данії – 70% [9]. Разом це зміщує бізнес-моделі до «компонувальних» підприємств, що збирають процеси з керованих і платформних сервісів, скорочуючи цикл виведення продуктів і підвищуючи стратегічну залежність від глобальних платформ. Для держав це означає нові компроміси між відкритістю інноваціям та контролем над критичною інфраструктурою й даними (табл. 1).

Таблиця 1

**Таксономія сегментів світового ринку ІТ-послуг і роль у цифровій трансформації**

| Сегмент                             | Ключова функція                                             | Типова модель експорту                       |
|-------------------------------------|-------------------------------------------------------------|----------------------------------------------|
| ІТ-консалтинг та архітектура        | стратегії, ТОМ, дорожні карти                               | дистанційно + короткі onsite-спринти         |
| Розробка ПЗ та інтеграція           | цифрові продукти, API/legacy інтеграції                     | offshore/nearshore команди, agile            |
| Керовані послуги (Managed Services) | безперервна підтримка, SRE, SLA                             | підписка, NOC/SOC 24/7                       |
| Хмарні та платформні сервіси        | міграція, DevOps/DevSecOps, multi-cloud                     | pay-as-you-go, віддалене адміністрування     |
| Дані, аналітика та AI               | дата-інженерія, MLOps, аналітика рішень                     | центри компетенцій                           |
| Кібербезпека як сервіс (MSSP)       | моніторинг загроз, Zero Trust, дотримання вимог (комплаєнс) | SOC-як-послуга                               |
| Інфраструктура й мережі             | ДЦ, мережі, edge/IoT                                        | гібрид: локальні інтегратори + гіперскейлери |

Джерело: сформовано авторами.

Світова карта ІТ-послуг формує кілька «ядер сили»: США, ЄС, Китай, Індія та вузли Південно-Східної Азії (передусім Сингапур) [6]. За даними COT, у 2024р. США були найбільшим окремим експортером комерційних послуг, тоді як ЄС як єдиний блок мав ще більші обсяги торгівлі з рештою світу – отже, трансатлантична пара задає темп ринку; Азія нарощує позиції за рахунок швидкого зростання «комп'ютерних послуг». ЄС у 2023р. лишився найбільшим у світі трейдером послуг загалом, що підтверджує його роль як регуляторного й комерційного центру тяжіння. Для країн, що розвиваються, ядро експорту послуг концентрується у Китаї, Індії, Сингапурі та ОАЕ – саме вони зібрали левову частку приросту у 2023 р.

Ринок хмарної інфраструктури – ключовий «важіль» впливу глобальних корпорацій, що диктує стандарти DevOps/AI та канали експорту ІТ-послуг. За оцінками ОЕСР, у низці найбільших економік ОЕСР сукупна частка двох гравців (Microsoft і Amazon) у хмарних сервісах сягала до 80%, що посилює бар'єри входу й залежність клієнтів. Позицію британського регулятора

підсилює фінальне рішення СМА (2025): фіксується концентрація, низькі темпи переходу між провайдерами та плани надати статус стратегічних ринкових гравців (SMS) для адресних інтервенцій [9].

ЄС інституціоналізує вплив через Digital Markets Act: визначає «gatekeepers» (Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft) і накладає на них обов'язки, що відкривають ринки комплементарним сервісам та зменшують «ефект замикання» для споживачів і бізнесу. Китай формує власний контур даних через PIPL (екстериторіальність, режими трансферу даних), що підвищує внутрішню керованість цифрового ринку та впливає на моделі надання ІТ-послуг нерезидентам.

Хмарні гіперскейлери та «воротарі» (gatekeepers) одночасно задають технічні стек-де-факто й контролюють канали дистрибуції: маркетплейси SaaS, API-екосистеми, identity-шари. Це зміщує додану вартість у бік платформи, де формується «плата за доступ» до попиту (трафік, білінг, дані), а для країн – питання цифрового суверенітету (табл. 2).

Таблиця 2

**Центри впливу на ринку ІТ-послуг: порівняльні переваги та регуляція**

| Центр                     | Рухії сили                                             | Регуляторний підхід / ринкові риси                                                |
|---------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------|
| США                       | гіперскейлери, R&D, глибокі ринки капіталу             | конкуренція ex-post, антимонопольні розслідування; висока приватна стандартизація |
| ЄС                        | масштаб попиту, інтегрований ринок, експорт правил     | DMA / gatekeepers, комплаєнс-вимоги як «експорт регуляції»                        |
| Китай                     | масштаб внутрішнього ринку, платформи, індустрполітика | PIPL, контроль даних/локалізація; внутрішня екосистема з обмеженим допуском       |
| Індія                     | експорт комп'ютерних послуг, кадри                     | курс на суверенітет даних; подальша імплементація правил DPDP (у контексті)       |
| Півд.-Сх. Азія (Сингапур) | фінансово-логістичний хаб, регіональні HQ              | про-інноваційне регулювання, угоди про цифрову торгівлю                           |

Джерело: сформовано авторами.

Цифровізація пришвидшує зростання ІТ-послуг, але водночас підсилює залежність від зовнішніх платформ, стандартів і постачальників. На рівні кіберзагроз картина загострюється: за ENISA у 2024 р. серед «праймівих» загроз домінували атаки на доступність (DDoS), далі – ransomware та інциденти з даними; найбільш уражені – публічне управління, транспорт, банківський сектор і цифрова інфраструктура. Для економічної безпеки це означає ризики переривання

критичних сервісів, істотних фінансових втрат і ланцюгових ефектів для суміжних галузей.

Крім технічної вразливості, формується регуляторно-ринкова залежність. За OECD, бар'єри для торгівлі послугами (включно з цифровими) у світі зросли на ~25% у 2014–2023 рр., зокрема через правила даних і вимоги до інфраструктури зв'язку. Обмеження транскордонних потоків даних мають відчутні макроефекти: спільні оцінки OECD/COT показують, що сценарій

«повної фрагментації» даних тягне втрати глобального ВВП на 4,5–5% (а також скорочення експорту на ~8,5%) [1]. Це прямо транслюється у втрату конкурентоспроможності секторів, що залежать від цифрово доставлених послуг і аналітики даних.

Окремий пласт – концентрація хмарної інфраструктури і «ефекти замикання». Підсумкове рішення регулятора Великої Британії (СМА, 2025) констатує, що конкуренція на ринку хмарних послуг «працює не належним чином»; серед причин – технічні та комерційні бар'єри перемикавання/мультисорсингу, а також практики ліцензування, що посилюють залежність клієнтів. Для держав і великих експортерів ІТ-послуг це підвищує ризик шоків у разі змін цін/умов або геополітичних обмежень постачальників.

Зростає і ризик ланцюгів постачання софту/послуг: ENISA фіксує, що інциденти з даними часто пов'язані з атаками на ланцюги поставок і соціальну інженерію

(зокрема Business Email Compromise), що множить наслідки – від простоїв до штрафів за порушення комплаєнсу. Для економічної безпеки критичними стають не лише фаєрволи, а й договірні та організаційні механізми: аудит постачальників, вимоги до розкриття інцидентів, можливість оперативної міграції між провайдерами.

Ще один виклик – екстериторіальність регулювання (правила даних, кіберзвітництва, контроль експорту технологій). Коли ключові канали надання ІТ-послуг проходять через юрисдикції з жорсткими режимами даних, країни-імпортери послуг отримують регуляторний ризик: зміна правил поза їхнім контролем впливає на доступність сервісів, вартість комплаєнсу й захист інвестицій. По суті, цифрова відкритість і безпека мають налаштовуватись одночасно, а не послідовно (табл. 3).

Таблиця 3

**Матриця ризиків цифрової залежності (чутливість для економічної безпеки)**

| Сегмент<br>(з таблиці 1) | Кіберризики | Ризик даних/ юрисдикцій | Vendor lock-in | Коментар до ризику                                        |
|--------------------------|-------------|-------------------------|----------------|-----------------------------------------------------------|
| Керовані послуги/ MSSP   | Високий     | Середній                | Середній       | Інцидент у провайдера множить на всіх клієнтів            |
| Хмара/ платформи         | Середній    | Високий                 | Високий        | Бар'єри перемикавання, ліцензування, інтероперабельність  |
| Дані та AI               | Середній    | Високий                 | Середній       | Транскордонні обмеження, комплаєнс, тренувальні набори    |
| Розробка та інтеграція   | Середній    | Середній                | Середній       | Залежність від стеків/SDK, ризики ланцюга постачання      |
| Інфраструктура/ мережі   | Середній    | Середній                | Середній       | «Точки відмови» в критичній інфраструктурі                |
| Консалтинг/ архітектура  | Низький     | Низький                 | Низький        | Ризик нижчий, але визначає вибір архітектур і провайдерів |

*Джерело:* сформовано авторами.

Вектор політики має прямо адресувати ризики, наведені у табл. 3: кіберзагрози, залежність від юрисдикцій даних і vendor lock-in, а також уразливість ланцюгів постачання. У ЄС системоутворюючим інструментом стала NIS2, що розширює коло критичних секторів, вводить обов'язки з управління ризиками та інцидент-репортування, а також посилює вимоги до supply chain security – це переводить безпеку ІТ-послуг у площину національної стійкості, а не суто ІТ-комплаєнсу. Паралельно Data Act встановлює правила переносимості та інтероперабельності даних/хмарних сервісів і захисні запобіжники проти доступу третіх країн до неф персональних даних усупереч праву ЄС; також передбачено поетапне усунення плати за «перемикавання» між провайдерами хмарних послуг.

*Перший шар – портованість і інтероперабельність даних.* Вектор політики має починатися з усунення бар'єрів для перенесення даних і сервісів між постачальниками, оскільки саме «залипання» в одному технологічному середовищі створює найглибші ризики цифрової залежності. Прийнятий у ЄС Data Act кодифікував право користувачів змінювати провайдера хмарних та обчислювальних послуг, поетапно скасовує плату за перемикавання (switching/egress charges) та запроваджує договірні exit-клаузи щодо

строків, форматів і артефактів перевірки. У поєднанні зі стандартами ISO/IEC та NIST це створює основу для технічної сумісності, зменшує транзакційні витрати при зміні постачальника й формує «страхувальну подушку» для державних і корпоративних клієнтів, які інтегруються в транскордонні ланцюги доданої вартості. Саме цей рівень забезпечує фундаментальну передумову для подальших шарів співпраці – від сертифікації до архітектур стійкості.

*Другий шар – сертифікація та стандарти.* На основі Cybersecurity Act ENISA розробляє європейські схеми сертифікації (рівні basic/substantial/high), покликані зробити вимоги прозорими для ІКТ-продуктів/послуг і зменшити асиметрію інформації на ринку. Розробка схеми EUCS (для хмар) триває; дискусія щодо її остаточної архітектури підкреслює баланс між безпекою і конкуренцією на ринку хмарних послуг.

*Третій шар – архітектури стійкості.* У США EO 14028 інституціоналізує вимоги до безпеки ланцюга постачання ПЗ і практик «secure-by-design», а NIST SP 800-207 (і 207A) задає операційну модель Zero Trust (зокрема для мултихмарних середовищ), що зменшує наслідки компрометації та латерал-руху атак. Для експортерів ІТ-послуг це ще й стандарт де-факто у

держзакупівлях.

*Четвертий шар – режими даних і трансгранична співпраця.* Для забезпечення законних трансферів персональних даних між ЄС і США ухвалено EU-US Data Privacy Framework (рішення про адекватність від 10.07.2023), що знижує регуляторну невизначеність для сервісів, які покладаються на трансатлантичні потоки. Для електронних доказів і взаємодії правоохоронних органів розроблено Другий додатковий протокол до Будапештської конвенції (CETS №224), який посилює механізми доступу до даних за кордоном та співпрацю в надзвичайних ситуаціях. Поза ЄС важливо, що Індія запровадила DPDP Act 2023, формуючи сучасний режим обробки персональних даних і закладаючи основу для сумісності з глобальними потоками.

*П'ятий шар – конкурентна політика щодо хмар.* Рішення СМА (UK, 2025) прямо ідентифікує бар'єри перемикання та практики ліцензування як фактори ринкової влади; регуляторні інтервенції (porting, інтероперабельність, обмеження anti-competitive bundling) – це вже не про «зручність IT», а про економічну безпеку

і стійкість ланцюгів послуг (табл. 4).

В основі прогнозу – два протилежні вектори й один проміжний: консолідація платформ, диверсифікація/регіоналізація та змішаний режим. У всіх трьох випадках попит на цифрово доставлені послуги зберігає динаміку, хоча темпи залежать від торговельної невизначеності та режимів даних. За оцінкою COT (квітневий Global Trade Outlook, 2025), у реальному вимірі торгівлі комерційними послугами зростає на 5,1% у 2025 р. і 4,8% у 2026 р. у базовому сценарії; у скоригованому з урахуванням тарифів та підвищеної невизначеності – на 4,0% та 4,1% відповідно. Цей «коридор» прогнозів і використовується нами для оцінювання стійкості сегментів ринку IT-послуг [1].

*Сценарій А – Консолідація платформ.* Рушієм виступає концентрація хмарної інфраструктури та каналів дистрибуції (маркетплейси SaaS, API-екосистеми). У Європі три провайдери акумулюють близько 70% ринку, а частка локальних гравців стабілізувалась біля 15%; це підвищує бар'єри перемикання та ризики vendor lock-in.

Таблиця 4

#### Заходи державної політики забезпечення економічної безпеки у сфері IT-послуг

| Політика/інструмент                      | Цільовий ризик                           | Приклади норм/стандартів              | Очікуваний ефект                                       |
|------------------------------------------|------------------------------------------|---------------------------------------|--------------------------------------------------------|
| Переносимість і інтероперабельність хмар | Vendor lock-in, безперервність           | Data Act (switching/interop)          | Зниження витрат перемикання, підвищення конкуренції    |
| Сертифікація безпеки послуг              | Асиметрія інформації, ланцюги постачання | Cybersecurity Act; схеми EUCS         | Порівнянність рівнів безпеки, довіра до постачальників |
| Управління ризиками й інцидент-репортинг | Системні збої, каскадні ефекти           | NIS2 (сектори, SCRM, повідомлення)    | Скорочення часу реакції, прозорість у ланцюгах         |
| Архітектура Zero Trust (мультихмара)     | Компрометація, латеральний рух           | NIST SP 800-207/207A, вимоги EO 14028 | Локалізація збитків, операційна стійкість              |
| Режими транскордонних даних              | Регуляторна невизначеність               | EU-US DPF (adequacy), DPDP (Індія)    | Правова визначеність для експортерів IT-послуг         |
| Правоохоронна кооперація                 | Кіберінциденти з іноземним елементом     | 2-й Протокол до Будапештської         | Швидший доступ до е-доказів, стримування загроз        |
| Конкурентні засоби на хмарному ринку     | Рентна залежність від гіперскейлерів     | CMA (UK) 2025                         | Стимул до porting/мульти-сорсингу                      |

Джерело: сформовано авторами.

Паралельно британський регулятор дійшов висновку, що конкуренція в хмарі «працює не належним чином», серед причин – технічні й комерційні бар'єри мультихмари та ліцензування. Для економічної безпеки країн та експортерів IT-послуг це означає вищу чутливість до цінових/договірних шоків і регуляторних рішень юрисдикцій-постачальників.

*Сценарій В – Диверсифікація/регіоналізація.* Паралельно посилюється тренд на регіональні цифрові простори та угоди про цифрову торгівлю. В АСЕАН ведуться переговори щодо DEFA з ціллю завершити їх до кінця 2025 р.; очікується гармонізація правил даних, електронної ідентифікації, кібербезпеки та міждержавних цифрових послуг. Для країн, що розвиваються, це шанс наростити експорт IT-послуг через регіональні платформи і взаємне визнання стандартів.

*Сценарій С – Змішаний режим (контрольована відкритість).* Поєднання глобальних платформ із національними/регіональними вимогами до локалізації

даних, інтероперабельності та сертифікації. З огляду на те, що транскордонні потоки даних одночасно критичні для бізнесу і регуляторно чутливі, країни оптимізують баланс між інноваційністю та суверенітетом – через правила перенесення даних, «портованість» хмари та узгоджені механізми доступу до е-доказів (табл. 5).

За UNCTAD, найбільшими експортерами послуг серед країн, що розвиваються, лишаються Китай, Індія, Сингапур, ОАЕ, Туреччина; у 2018–2023 рр. найвищі темпи зростання експорту телекомунікаційних, комп'ютерних та інформаційних послуг фіксувались в Азії (у середньому ~14% на рік).

Додатковим каталізатором буде AI-інфузія: за МВФ, за умов правильної політики ІШ може прискорити продуктивність і створити додатковий попит на IT-послуги по всій економіці [9].

Таблиця 5

## Сценарії розвитку світового ринку IT-послуг: драйвери, ризики та політичні пріоритети

| Сценарій                          | Драйвери                                            | Ключові ризики для екон. безпеки                       | Політичні пріоритети                                  |
|-----------------------------------|-----------------------------------------------------|--------------------------------------------------------|-------------------------------------------------------|
| А. Консолідація платформ          | масштаб гіперскейлерів, AI-попит                    | lock-in, рентна залежність, екстериторіальність рішень | портованість/ інтеперабельність, конкуренційні засоби |
| В. Диверсифікація/ регіоналізація | DEFA/угоди про цифрову торгівлю, регіональні хмари  | фрагментація ринків, дублювання вимог                  | взаємне визнання стандартів, «легкі» потоки даних     |
| С. Змішаний режим                 | поєднання глобальних платформ і нац./регіон. правил | складність комплаєнсу, координаційні витрати           | risk-based підхід до даних, мультимедіа, сертифікація |

Джерело: сформовано авторами.

Консолідація зручна для швидкого масштабування, але підвищує системні ризики; регіоналізація знижує залежність, але загрожує «фрагментацією» ринків і зменшенням ефекту масштабу. Політики на кшталт інтеперабельності й «портованості» хмар, а також узгоджених режимів даних, формують контрольовану відкритість, яка мінімізує ризики без втрати зростання.

**Висновки.** Світовий ринок IT-послуг став опорною інфраструктурою цифрової економіки: саме через послуги відбувається безперервна модернізація бізнес-процесів і державних сервісів, а додана вартість дедалі частіше концентрується на рівні платформ та правил. Гео економічно ринок організований навколо кількох центрів сили (США, ЄС, Китай, Індія, Сингапур/АСЕАН), де поєднання технологічної концентрації та «експорту регуляцій» формує асиметрії доступу до попиту, даних і стандартів. Паралельно з очевидними вигодами для продуктивності зростають уразливості економічної безпеки: кіберзагрози, юрисдикційні ризики обігу даних, vendor lock-in у хмарній інфраструктурі, а також ризики ланцюгів постачання ПЗ і

послуг. Оптимальна відповідь не зводиться до дилеми «відкритість або контроль»: потрібна контрольована відкритість, у якій інтеперабельність і портованість сервісів, сертифікація й керування ризиками, архітектури Zero Trust та конкурентна політика на ринку хмар поєднуються з правовою визначеністю транскордонних потоків даних. Сценарний аналіз показує, що крайнощі – тотальна консолідація платформ або глибока регіоналізація – несуть або системну залежність, або фрагментацію ринків; найбільш життєздатним видається змішаний режим, що підтримує інновації та масштаб, але стримує рентну залежність і переносить стійкість у центр державної політики. Для відкритих і перехідних економік це означає пріоритет мультимедіа, розвитку дано-інфраструктури, участі в цифрових угодах і посилення вимог до безпеки та прозорості постачальників; для експортерів IT-послуг – здатність працювати у багатоюрисдикційному середовищі з вбудованою кіберстійкістю та дотриманням вимог регуляторних режимів.

## Список використаних джерел:

1. Economic Implications of Data Regulation. (2025). WTO. URL: [https://www.wto.org/english/res\\_e/booksp\\_e/data\\_regulation\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf)
2. Global Trade Outlook and Statistics. (2024). WTO. URL: [https://www.wto.org/english/res\\_e/booksp\\_e/trade\\_outlook24\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/trade_outlook24_e.pdf)
3. Guo, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation? Computer Law & Security Review, Vol. 56. Article 106079. URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4806703](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806703)
4. Gupta, S., Ghosh, P., & Sridhar, V. (2022). Impact of data trade restrictions on IT services export: A cross-country analysis. Telecommunications Policy, Vol. 46. Iss. 9. Article 102403. DOI: <https://doi.org/10.1016/j.telpol.2022.102403>
5. Herman, P.R., & Oliver, S. (2023). Trade, policy, and economic development in the digital economy. Journal of Development Economics, Vol. 164. Article 103135. DOI: <https://doi.org/10.1016/j.jdevec.2023.103135>
6. Honcharenko, V., Panteleimonenko, A., Pozhar, A., & Stetsenko, V. (2019). Cooperatives in IT sector: theoretical and practical aspects. Periodicals of Engineering and Natural Sciences, Vol. 7(2). Pp. 597-607. DOI: <https://doi.org/10.21533/pen.v10.i1.570>
7. Li, H., Han, J., & Xu, Y. (2023). The effect of the digital economy on services exports competitiveness and ternary margins. Telecommunications Policy, Vol. 47. Iss. 7. Article 102596. DOI: <https://doi.org/10.1016/j.telpol.2023.102596>
8. Shaik, V., & Natarajan, K. (2024). Cloud databases: A resilient and robust framework to dissolve vendor lock-in. Software Impacts, Vol. 21. Article 100680. DOI: <https://doi.org/10.1016/j.simpa.2024.100680>
9. Handbook of Statistics 2024. (2025). UNCTAD. URL: <https://unctad.org/publication/handbook-statistics-2024>
10. Zhang, Y., Xu, J., Yang, W. (2024). Analysis of the evolution characteristics of international ICT services trade based on complex network. Telecommunications Policy, Vol. 48. Iss. 3. Article 102697. DOI: <https://doi.org/10.1016/j.telpol.2023.102697>

**References:**

1. Economic Implications of Data Regulation. (2025). WTO. Retrieved from: [https://www.wto.org/english/res\\_e/booksp\\_e/data\\_regulation\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf)
2. Global Trade Outlook and Statistics. (2024). WTO. Retrieved from: [https://www.wto.org/english/res\\_e/booksp\\_e/trade\\_outlook24\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/trade_outlook24_e.pdf)
3. Guo, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation? Computer Law & Security Review, Vol. 56. Article 106079. Retrieved from: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4806703](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806703) [in English].
4. Gupta, S., Ghosh, P., & Sridhar, V. (2022). Impact of data trade restrictions on IT services export: A cross-country analysis. Telecommunications Policy, Vol. 46. Iss. 9. Article 102403. DOI: <https://doi.org/10.1016/j.telpol.2022.102403> [in English].
5. Herman, P.R., & Oliver, S. (2023). Trade, policy, and economic development in the digital economy. Journal of Development Economics, Vol. 164. Article 103135. DOI: <https://doi.org/10.1016/j.jdeveco.2023.103135> [in English].
6. Honcharenko, V., Panteleimonenko, A., Pozhar, A., & Stetsenko, V. (2019). Cooperatives in IT sector: theoretical and practical aspects. Periodicals of Engineering and Natural Sciences, Vol. 7(2). Pp. 597-607. DOI: <https://doi.org/10.21533/pen.v10.i1.570> [in English].
7. Li, H., Han, J., & Xu, Y. (2023). The effect of the digital economy on services exports competitiveness and ternary margins. Telecommunications Policy, Vol. 47. Iss. 7. Article 102596. DOI: <https://doi.org/10.1016/j.telpol.2023.102596> [in English].
8. Shaik, V., & Natarajan, K. (2024). Cloud databases: A resilient and robust framework to dissolve vendor lock-in. Software Impacts, Vol. 21. Article 100680. DOI: <https://doi.org/10.1016/j.simpa.2024.100680> [in English].
9. Handbook of Statistics 2024. (2025). UNCTAD. Retrieved from: <https://unctad.org/publication/handbook-statistics-2024> [in English].
10. Zhang, Y., Xu, J., Yang, W. (2024). Analysis of the evolution characteristics of international ICT services trade based on complex network. Telecommunications Policy, Vol. 48. Iss. 3. Article 102697. DOI: <https://doi.org/10.1016/j.telpol.2023.102697> [in English].