DOI: https://doi.org/10.32782/2524-0072/2025-78-19

УДК 339.9:004.738.5(100)+338.24.021.8

МІЖНАРОДНА КООПЕРАЦІЯ В СФЕРІ ІТ-ПОСЛУГ ЯК ДРАЙВЕР ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВ

INTERNATIONAL COOPERATION IN IT SERVICES AS A DRIVER OF NATIONAL ECONOMIC SECURITY

Гончаренко Владислав Васильович
доктор економічних наук, професор,
Харківський національний університет імені В. Н. Каразіна
ORCID: https://orcid.org/0000-0002-0414-8892

Зайцева Анна Сергіївна
доктор економічних наук,
Харківський національний університет імені В. Н. Каразіна
ORCID: https://orcid.org/0000-0003-0818-7853

Пожар Артем Анатолійович
кандидат економічних наук, доцент,
Полтавський університет економіки і торгівлі
ORCID: https://orcid.org/0000-0002-8662-9074

Honcharenko Vladyslav, Zaitseva Anna
V. N. Karazin Kharkiv National University

Pozhar Artem
Poltava University of Economics and Trade

Стаття досліджує міжнародну кооперацію в ІТ-послугах як інструмент зміцнення економічної безпеки держав. Запропоновано модель «контрольованої відкритості», що поєднує правові гарантії портованості, технічну інтероперабельність та сертифікаційно-операційні механізми довіри. На основі типології угод, спільних рамок кіберзахисту й кооперaційної дано-інфраструктури показано, як зменшуються vendor lock-in і ризики ланцюгів постачання, підвищуються стійкість і передбачуваність транскордонних потоків даних. Сформовано «матрицю» відповідності режимів і стандартів та дорожню карту для країн із перехідною економікою (портованість, мапінги ISO/NIST, сертифікація, CSIRT/ISAC, дипломатія правил). Практична цінність – у поетапному впровадженні політик, що розширюють експортні спроможності ІТ-сектора без втрати інноваційної динаміки.

Ключові слова: міжнародна кооперація, ІТ-послуги, економічна безпека, портованість, інтероперабельність, кібербезпека, сертифікація, транскордонні потоки даних, цифровий суверенітет.

The paper examines international cooperation in IT services as a driver of national economic security and develops a model of controlled openness that integrates three complementary layers: legal guarantees of portability enabling provider switching and cross-border transfer; technical interoperability grounded in widely adopted reference models and standards; and certification- and operations-oriented assurance that renders trust verifiable across service supply chains. The topic is timely because digitalization concentrates platform power, fragments data regimes, and elevates cyber risks, jointly amplifying vendor lock-in and regulatory uncertainty for open and transition economies. Methodologically, the study combines structured review, comparative policy analysis, standards mapping, and conceptual synthesis. We classify cooperation instruments (bilateral and plurilateral digital economy agreements and public–private alliances), systematize joint cybersecurity practices (CSIRT/ISAC networks, incident information sharing, joint exercises, and certification schemes), and frame technology and data-infrastructure options (shared or "sovereign" clouds with portability and interoperability profiles). Building on these blocks, we construct a matrix that links legal grounds for data transfers with assurance frameworks and security/privacy management standards, and derive a stepwise roadmap tailored to transition economies. Results show that coordinated portability and interoperability reduce vendor lock-in and bargaining asymmetries, while joint cyber capabilities and aligned certification shorten detection and response times and lower transaction costs along cross-border service chains. The matrix clarifies how legal transfer bases align with assurance and management standards, supporting predictable international

data flows without undue market fragmentation. The practical contribution is an implementation-ready toolkit for policymakers and international partners to operationalize controlled openness: it preserves innovation dynamics and market access while strengthening resilience, enabling multi-sourcing, and expanding export capabilities in IT services; the modular framework is adaptable to diverse institutional settings and can be monitored using clear progress indicators.

Keywords: international cooperation, IT services, economic security, portability, interoperability, cybersecurity, certification, cross-border data flows, digital sovereignty.

Постановка проблеми. Стрімка цифровізація перетворила ринок IT-послуг на опорну інфраструктуру економіки, однак зростання супроводжується концентрацією платформ, «приватною» стандартизацією, фрагментацією режимів обігу даних і ескалацією кіберризиків. Це породжує асиметрії доступу до технологій, vendor lock-in і підвищує транскордонні операційні ризики, особливо для відкритих і перехідних економік. Існуючі підходи здебільшого розглядають хмару, конкуренцію та політики даних роз'єднано; бракує інтегрованої геоекономічної рамки, що пов'язує структуру глобального ринку, правила обігу даних і канали передачі ризиків між сегментами послуг. Політика «контрольованої відкритості» – портованість і інтероперабельність даних/хмар (механізми типу Data Act), мультіхмара та мультісорсинг, сертифікація і Zero Trust, доповнені конкуренційними інструментами у хмарному сегменті – зменшує системну залежність і регуляторну невизначеність без втрати темпів інновацій. Оптимальна траєкторія для більшості економік – змішаний режим, що поєднує глобальні платформи з національними/регіональними вимогами.

Аналіз останніх досліджень і публікацій. Сучасна література підтверджує, що правила даних і цифрова зрілість економік істотно визначають траєкторії торгівлі IT-послугами. Gupta, Ghosh і Sridhar показують, що обмеження транскордонних потоків даних статистично знижують експорт IT-послуг (індекс MDRI як міра «жорсткості» політик) [5]. Li, Han та Xu фіксують, що розвиток цифрової економіки підвищує конкурентоспроможність експорту послуг через інтенсивну й екстенсивну маржі [8]. Мережевий аналіз Zhang, Xu та Yang ідентифікує структурну концентрацію зв'язків у торгівлі ІКТ-послугами (2004–2020), висвітлюючи ядро та канали інтеграції [9]. На макрорівні Herman і Oliver показують, що положення про цифрову торгівлю та інтернет-зв'язність підсилюють товарні й сервісні потоки та добробут, фактично стимулюючи «експорт правил» [6]. Регуляторна практика Китаю за Guo і Li демонструє перехід від жорстких до гнучкіших режимів трансферу даних, що знижує транзакційні витрати для цифрової торгівлі [4].

Виділення невирішених раніше частин загальної проблеми. Попри ці результати, залишається брак інтегрованої рамки, яка одночасно поєднала б політики даних (adequacy/SCC/BCR), сертифікаційні стандарти та портованість/ інтероперабельність як єдиний механізм зміцнення економічної безпеки у транскордонних IT-екосистемах.

Формулювання цілей статті (постановка завдання). Мета статті – обґрунтувати та операціоналізувати рамку міжнародної кооперації в IT-послугах як інструмент зміцнення економічної безпеки держав. Для цього систематизуються форми співпраці (бі-/плюрилатеральні угоди, DEAs, публічно-приватні альянси), спільні механізми кіберзахисту (CSIRT/ISAC, обмін індикаторами, сертифікація), а також технологічні та дано-інфраструктурні рішення (суверенні/спільні хмари, інтероперабельність, портованість). Мета передбачає зіставлення регуляторних режимів транскордонних потоків даних (adequacy/DPF, SCC/BCR, CBPR, стандарти ISO/IEC, NIST) і формування моделі «контрольованої відкритості», що поєднує правові, технічні та сертифікаційно-операційні контури довіри. На цій основі пропонується дорожня карта для країн із перехідною економікою (правові гарантії портованості, стандарти/мапінги, сертифікація, інституційні спроможності, дипломатія правил), спрямована на зменшення *vendor lock-in*, підвищення стійкості та розширення експортних спроможностей IT-послуг.

Виклад основного матеріалу дослідження. Міжнародна кооперація в IT-послугах [10] сформувалася як багаторівнева архітектура правил і практик, що поєднує юридично зобов'язальні угоди, «м'які» рамки довіри до даних, операційні мережі реагування та спільні інфраструктурні ініціативи [7] (рис. 1).

На верхньому (першому) рівні перебувають угоди цифрової економіки (DEAs), які фіксують норми щодо транскордонних потоків даних, електронної ідентифікації, електронних рахунків-фактур та кооперативні модулі (AI/fintech/regtech). Показовими є DEPA

Рис. 1. Типологія міжнародної кооперації в IT-послугах

Джерело: розроблено авторами

(Сінґапур–Нова Зеландія–Чилі) із процедурою приєднання й Протоколом, що підсилив юридичну визначеність правил (набрав чинності 19.03.2024), а також приєднання Республіки Корея 03.05.2024 як першого нового члена. Аналогічну логіку демонструє UK–Singapore DEA, що набув чинності 14.06.2022 і поєднав обов'язкові дисципліни щодо потоків даних із кооперацією в штучному інтелекті, фінтеху та цифрових ідентичностях, а також Australia–Singapore DEA (в силі з 08.12.2020) як ранній зразок «цифрових» положень двосторонньої торгівельної архітектури [1].

Другий шар становлять рамки довіри до даних, які забезпечують інтероперабельність режимів приватності та знижують транзакційні витрати для цифрової торгівлі. Концепт G7 Data Free Flow with Trust (DFFT), сформульований на G20 Osaka (2019) і операціоналізований у 2023 р. через Institutional Arrangement for Partnership, слугує політичною «парасолькою» для впровадження довірених потоків даних. У трансатлантичному вимірі діє EU–US Data Privacy Framework – рішення ЄК про «адекватність» (Implementing Decision (EU) 2023/1795 від 10.07.2023), що легалізує передання персональних даних з ЄЕП до США для сертифікованих компаній. У ширшому колі юрисдикцій сертифікаційний підхід розвиває Global CBPR Forum, створений 2022 р. як наступник APEC CBPR для глобального узгодження стандартів приватності й довіри [2].

Третій шар – операційна кіберкооперація. В ЄС мережа CSIRTs за участю ENISA, заснована Директивою NIS та посилена NIS2, забезпечує координацію інцидентів і обмін індикаторами компрометації між національними командами, включно з CERT-EU. На глобальному рівні до взаємодії долучаються галузеві ISAC-платформи та багатосторонні форуми реагування; кримінально-правовий вимір підтримує Будапештська конвенція про кіберзлочинність, що уніфікує матеріальні склади правопорушень і механізми взаємної допомоги та прискорених запитів даних між компетентними органами.

Четвертий шар становлять стандарти й сертифікація безпеки (наприклад, схеми EU Cybersecurity Certification: EUCC на основі Common Criteria та проєкт EUCS для хмарних сервісів), які підвищують прозорість ланцю-

гів постачання, полегшують взаємне визнання вимог і створюють передбачуване регуляторне поле для постачальників IT-послуг. Нарешті, інфраструктурний шар представлений спільними дата-ініціативами на кшталт Gaia-X, що встановлюють федеративні правила інтероперабельності, портованості та прозорості, дозволяючи будувати «суверенні» хмарні рішення без втрати доступу до глобальних ринків. У сукупності ці шари формують матрицю кооперації, яка зменшує ризики цифрової залежності (vendor lock-in, юрисдикційні бар'єри, кіберзагрози), пришвидшує інтеграцію постачальників у транскордонні ланцюги створення вартості та, зрештою, слугує інструментом зміцнення економічної безпеки держав [3].

Інституційна співпраця у сфері кіберзахисту переходить від декларативних принципів до операційної взаємодії, що безпосередньо знижує системні ризики для транскордонних IT-послуг і підсилює економічну безпеку. На рівні ЄС мережа CSIRTs (національні команди реагування на комп'ютерні інциденти) діє у спільних процедурах виявлення та реагування, координованих ENISA; оновлена директива NIS2 розширила охоплення критичних секторів, гармонізувала вимоги до повідомлення про інциденти та передбачила поглиблений обмін технічними даними між державами-членами. Паралельно в публічно-приватному вимірі функціонують ISACs – галузеві центри обміну та аналізу інформації, які створюють «контури довіри» для швидкого поширення індикаторів компрометації й найкращих практик між бізнесом і органами влади; в ЄС їх розвиток підтримує ENISA, а в США координацію здійснює National Council of ISACs [2].

Ключову роль у підвищенні спроможності систем відіграють спільні навчання: цикл Cyber Europe випробовує міжвідомчу координацію та процедурну сумісність на тлі сценаріїв комплексних інцидентів, а Locked Shields (під егідою CCDCOE) забезпечує стрес-тестування технічної готовності до атак на критичну інфраструктуру та ланцюги постачання. Для узгодженого обміну телеметрією та артефактами атак дедалі ширше застосовують відкриті формати STIX/TAXII, що зменшує затримки між виявленням і колективним реагуванням у багатодержавних середовищах. Важливим елементом довіри у ланцюгах постачання є сертифікація: у межах EU Cybersecurity Certification Framework опубліковано схему EUCC (на основі Common Criteria) для ІКТ-продуктів, а також опрацьовується EUCS для хмарних сервісів; такі схеми полегшують взаємне визнання вимог, трансфер доказів відповідності та зниження транзакційних витрат для провайдерів і замовників IT-послуг. Поза ЄС операційні зв'язки підтримують FIRST (глобальна спільнота команд реагування) і регіональні платформи (TF-CSIRT, APCERT), що розширює охоплення спільних стандартів у позаєвропейських юрисдикціях.

Сукупність цих інструментів утворює багатоконтурну архітектуру співпраці: від нормативної сумісності й уніфікованих форматів даних до сталих каналів обміну індикаторами та верифікованих рівнів гарантій безпеки. У практичному вимірі це скорочує час детекції та реагування, підвищує прозорість постачальників і знижує ризики ланцюгів постачання, що є необхідною умовою довіри до транскордонних IT-сервісів (таблиця 1).

Таблиця 1

Інструменти кіберкооперації та відповідні типи ризиків

Інструмент співпраці	Тип(и) ризику, на який націлено
Мережі CSIRT (ENISA/ЄС; TF-CSIRT; APCERT)	Масштабні інциденти, збої критичної інфраструктури, транскордонні ланцюжки атак
ISACs (галузеві центри)	Секторні кампанії (ransomware, фішинг), швидкий обмін TTP/IoC між бізнесом і державою
Спільні навчання (Cyber Europe; Locked Shields)	Координація реагування, випробування процедур, атаки на енергетику, фінанси, зв'язок
Обмін індикаторами (STIX/TAXII)	Затримки детекції, фрагментація форматів, помилки кореляції подій
Сертифікація (EUCC; EUCS – хмарні сервіси)	Ризики постачальників і сумісності, прогалини комплаєнсу, довіра в ланцюгах постачання
Глобальні спільноти реагування (FIRST)	Синхронізація реакції на глобальні кампанії (DDoS, supply-chain), поширення попереджень

Джерело: розроблено авторами

Інфраструктурний вимір кооперації в IT-послугах [11] поступово переходить від «віртуальних» домовленостей до матеріалізованих архітектур даних і хмар. На тлі посилення регуляторних вимог у ЄС саме інтероперабельність і портованість визначають життєздатність спільних проєктів та їхню відповідність стратегічним пріоритетам економічної безпеки. Data Act кодифікує право клієнта змінювати провайдера «data processing services» і встановлює поетапне вилучення плати за перемикання (включаючи data egress): з 12 січня 2027 р. такі switching charges заборонені, а більшість обов'язків щодо перемикання діятимуть з 12 вересня 2025 р. Ці норми створюють економічний стимул до мультіхмарності та знижують ризик vendor lock-in, що є ключовим для транскордонних сервісів і державних замовників [1].

Технічну сторону «контрольованої відкритості» задають стандарти та референс-моделі. ISO/IEC 19941 прямо визначає поняття інтероперабельності та портованості у хмарних середовищах (класи портованості, сценарії перенесення сервісів/даних), а NIST SP 500-292 описує ролі та інтерфейси (споживач, провайдер, брокер, аудитор, перевізник), що дозволяє проектувати багатосторонні схеми з чіткими зонами відповідальності. Спирання на ці описи мінімізує транзакційні витрати при зміні постачальника й полегшує договірне закріплення exit-клауз (терміни, формати, артефакти перевірки). У європейській практиці цей технічний пласт перегукується з підходами Gaia-X до федеративних правил і прозорості послуг (каталоги, декларації відповідності, політики перенесності), завдяки чому можливі «суверенні» рішення без відриву від глобальних екосистем.

Другий опорний контур – сертифікація кібербезпеки хмар. У ЄС розгортається EU Cybersecurity Certification Framework: схема EUCC (на основі Common Criteria) вже надає узгоджені рівні гарантій для ІКТ-продуктів, тоді як EUCS покликана гармонізувати вимоги саме до хмарних сервісів і полегшити їх транскордонне прийняття. Дискусія навколо «суверенітетних» критеріїв у проєкті EUCS у 2024–2025 рр. рухається в бік домінування технічних вимог над юрисдикційними, що, з одного боку, зберігає конкуренцію та вибір для замовника, а з іншого – вимагає від операційних проєктів додаткових контрактних та криптографічних запобіжників (локалізація ключів, шляхи підтримки on-prem/edge, escrow артефактів). Для державних клієнтів така конфігурація означає можливість вибудовувати «суверенну» експлуатацію поверх інтероперабельної багатохмарної основи.

У підсумку модель «контрольованої відкритості» (рис. 2) поєднує:

і) регуляторні гарантії портованості (клаузи перемикання з Data Act і поетапне скасування switching charges); іі) стандартизовані інтерфейси та формати на базі ISO/IEC та NIST-моделей, щоб фізично забезпечити переносимість і взаємодію; ііі) сертифікаційні та операційні гарантії (EUCC/EUCS, процедури безпечного виходу та прийому, перевірка журналів/артефактів). Для транснаціональних кооперацій – спільних дата-центрів, «суверенних» регіонів у гіперскейлерів, публічно-приватних дата-платформ – це означає, що відкритість керована: взаємодія можлива без втрати контролю над даними, а зміна постачальника – без руйнації сервісу. Саме така архітектура мінімізує системні ризики і підсилює стійкість ланцюгів постачання IT-послуг у геоекономічно чутливому середовищі.

Транскордонні потоки даних у сфері IT-послуг спираються на узгодженість правових режимів приватності та безпеки. У праві ЄС базовим механізмом є рішення про адекватність (adequacy), що дозволяє вільний рух даних до юрисдикцій із «сутнісно еквівалентним» рівнем захисту (Японія, Республіка Корея, Велика Британія тощо). Для США діє EU–US Data Privacy Framework (DPF), схвалений Рішенням Комісії (EU) 2023/1795; у 2025 р. Загальний суд ЄС відхилив позов проти DPF, що підвищило регуляторну визначеність для компаній-експортерів IT-послуг. Якщо ж адекватності немає, застосовують стандартні договірні положення (SCCs) або внутрішньокорпоративні правила (BCRs) – інструменти контрактної еквівалентності, які вимагають техніко-організаційних гарантій і процедур оцінки ризиків трансферу.

Паралельно розвиваються позарегіональні рамки «сертифікаційної еквівалентності», зокрема Global CBPR Forum, що надає механізм взаємного визнання приватнісних вимог для бізнесу в АТР та Північній Америці й декларує сумісність із DFFT-підходом («вільний рух даних із довірою»). На боці організаційних/технічних стандартів критичною є зв'язка ISO/IEC 27001 (ISMS) та ISO/IEC 27701 (PIMS), доповнена ISO/IEC 27017 (контролі безпеки для хмар) і ISO/IEC 27018 (захист PII у публічній хмарі); ця «сім'я» забезпечує передачність практик безпеки й приватності між провайдерами та юрисдикціями. Для управління кібер-

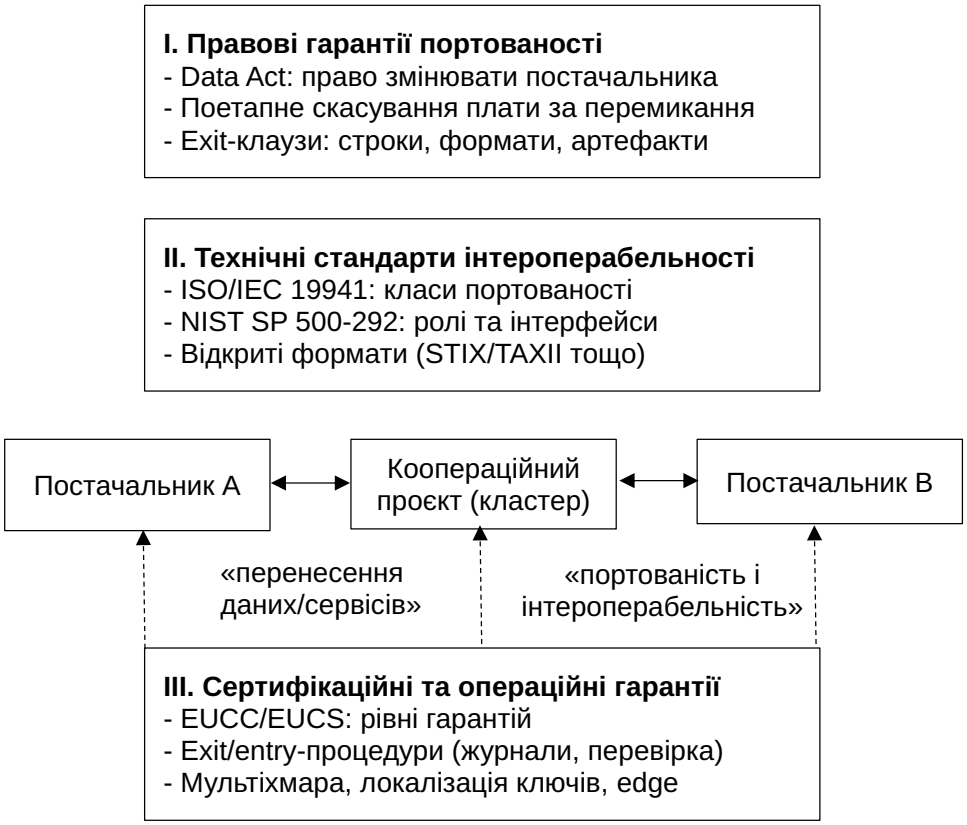

Рис. 2. Модель «контрольованої відкритості» для кооперaційних проєктів

Джерело: розроблено авторами

ризиками як «метастандарт» дедалі ширше використовується NIST CSF 2.0 (із доданою функцією Govern), який легко картографується на ISO-контроли й слугує мостом між різними системами регулювання. В ЄС роль «гаранта довіри» у ланцюгах постачання посилюють схеми сертифікації в межах EU Cybersecurity Certification Framework – EUCC (на основі Common Criteria) та підготовлювана EUCS для хмарних сервісів.

Рух до інтероперабельної глобальної екосистеми відбувається також через узгодження принципів державного доступу: OECD Declaration on Government Access to Personal Data (2022) кодифікує спільні засади пропорційності, нагляду й правового захисту, що знижує невизначеність для міжнародних трансферів і підсилює ініціативу DFFT. Сукупно ці інструменти формують «матричну» модель еквівалентності: правові підстави (adequacy/DPF/SCCs/BCRs), сертифікаційно-процесуальні рамки (CBPR, EUCC/EUCS), а також стандарти управління безпекою й приватністю (ISO/IEC, NIST) забезпечують взаємодоповнювані контури довіри для постачальників і споживачів IT-послуг у транскордонних сценаріях (таблиця 2).

Кооперaційні режими, описані вище, безпосередньо трансформують профіль економічної безпеки. По-перше, портованість і інтероперабельність зменшують *vendor lock-in*: *Data Act* кодифікує право змінювати провайдера хмарних/обчислювальних послуг, передбачає поетапне скасування *switching/egress charges* та закріплює *exit-клаузи* (терміни, формати, артефакти перевірки). Це вирівнює переговорну позицію замовників, робить мультісорсинг економічно доцільним і зменшує залежність від окремих юрисдикцій. По-друге, операційна стійкість зростає завдяки гармонізації вимог кіберзахисту: *NIS2* розширює перелік критичних секторів, підвищує стандарти звітності й взаємодії CSIRT, що скорочує час виявлення/реагування на інциденти у транскордонних ланцюгах постачання послуг. По-третє, сертифікаційні схеми (EUCC та кандидат EUCS) знижують транзакційні витрати на доведення відповідності та полегшують взаємне визнання рівнів гарантій безпеки – передумову доступу до регіональних

ринків у режимі «довіри за замовчуванням». Для країн із перехідною економікою системний ефект проявляється у зменшенні системних ризиків (одиничні «точки відмови», юрисдикційні пастки, *supply-chain* уразливості) та розширенні експортного фронтиру для ІТ-послуг. Довіра до практик безпеки/приватності (ISO/IEC 27001/27701/27017/27018 у зв'язці з NIST CSF 2.0) зменшує бар'єри входу для *offshore/nearshore* команд і керованих сервісів.

На макрорівні динаміка торгівлі послугами, які доставляються цифрово, підтверджує, що відповідність глобальним правилам і стандартам підсилює експорт спроможностей постачальників із країн, що наздоганяють (за рахунок як інтенсивної, так і екстенсивної маржі). Євростат фіксує помітну частку ІКТ-сектору у ВДВ ЄС (5,5% у 2022 р.), де домінують саме послуги – індикатор того, що політики довіри безпосередньо корелюють із вкладом сектора у зростання. Нарешті, участь у багатосторонніх ініціативах DFFT/IAP створює канали для взаємного визнання процедур і практик, знижуючи регуляторну невизначеність транскордонних потоків даних.

Політичний інструментарій для урядів має бути матричним: (i) правові гарантії портованості/доступу до даних (гармонізація з *Data Act*-підходом); (ii) впровадження стандартів і мапінгів (ISO/IEC ↔ NIST CSF 2.0); (iii) сертифікація/аудит (EUCC/EUCS або їхні еквіва-

Таблиця 2

Матриця відповідності режимів/стандартів для транскордонних потоків даних

Режим / стандарт	Правова підстава трансферу	Приватність (PIMS)	Безпека (ISMS/ контр.)	Нагляд/редрес	Взаємне визнання / інтероперабельність
GDPR Adequacy	Так (рішення ЄК)	–	–	Національні наглядові органи	Визнання між ЄС та «адекватними» країнами
EU–US DPF	Так (спеціальний режим)	Обов'язки учасників DPF	Контроли за програмою	DPRC/нагляд у США	Специфічна сумісність ЄС–США
SCCs / BCRs	Договірна еквівалентність	Вимоги до PII у договорах/ BCR	Технічні та організаційні заходи	Контроль НО + внутрішні механізми	Широка застосовність (за контрактом)
Global CBPR	Сертифікація ↔ трансфери	Принципи приватності	–	Акредитовані органи оцінки	Механізм взаємного визнання в учасників
ISO/IEC 27701	–	PIMS (розширення ISO 27001)	Узгоджені з ISMS контролі	Аудит/ сертифікація	Легко картографується на GDPR/CBPR
ISO/IEC 27001/17/18	–	27018 для PII у хмарі	ISMS (27001) + хмарні контролі (27017)	Аудит/ сертифікація	Сумісні з NIST CSF/ін. фреймворками
NIST CSF 2.0	–	Категорії Privacy (перетин)	Функції Identify–Recover + Govern	Добровільні керівні настанови	Використовується для мапінгу на ISO/ЄС
OECD Declara-tion	Принципи, не правова підстава	Захист прав	Гарантії пропорційності	Демокр. нагляд/ засоби прав. захисту	Підтримує DFFT, підвищує довіру

Джерело: розроблено авторами

Примітка до таблиці: «–» означає, що інструмент сам по собі не створює правової підстави для трансферу, але може бути використаний для доведення еквівалентності практик (через сертифікацію/аудит) або як опорний стандарт при контрактуванні (SCCs/BCRs).

ленти); (iv) інституційні спроможності (CSIRT/ISAC, процедури обміну індикаторами) у руслі *NIS2*; (v) дипломатія правил (участь у DFFT/IAP, дво-/плюрилатеральні модулі щодо даних). Дорожня карта нижче агрегує ці інструменти за етапами реалізації для країн із перехідною економікою (таблиця 3).

Висновки. У статті показано, що міжнародна кооперація в IT-послугах еволюціонує до архітектури «контрольованої відкритості», де правові гарантії портованості, технічні стандарти інтероперабельності та сертифікаційно-операційні механізми утворюють взаємодоповнювані контури довіри. У такій конфігурації Data Act знімає бар'єри перемикання та задає вимоги до *exit*-процедур; зв'язка ISO/IEC та NIST CSF 2.0 забезпечує перенесність даних/сервісів і сумісність процесів; схеми EUCC/EUCS переводять «довіру» у верифіковані рівні гарантій. Паралельно мережі CSIRT/ISAC, навчання та стандартизовані формати обміну індикаторами скорочують час детекції й реагування, зменшуючи системні ризики транскордонних ланцюгів постачання. Регуляторна еквівалентність і механізми взаємного визнання (рішення про адекватність, EU–US DPF, SCC/BCR, Global CBPR, принципи DFFT/OECD) формують «матрицю» правил, яка підсилює передбачуваність міжнародних потоків даних без надмірної фрагментації ринку.

Для країн із перехідною економікою запропонована дорожня карта демонструє, що поєднання правових, технічних і інституційних інструментів зменшує *vendor lock-in*, підвищує стійкість (через мультісорсинг, резервування, *edge/on-prem* інтеграції) та розширює експортний фронтир керованих IT-сервісів. Практична цінність підходу полягає у можливості поетапного впровадження: від «білої книги» портованості й типових *exit*-клауз до сертифікації провайдерів і участі в DFFT/IAP-механізмах. Науковий внесок статті – у формалізації тришарової моделі кооперації та «матричної» відповідності режимів/стандартів, що дозволяє оцінювати політики з позиції економічної безпеки, а також у пропозиції інструментарію для країн, що наздоганяють. Подальші дослідження доцільно спрямувати на кількісну валідацію ефектів портованості та сертифікації для експорту IT-послуг і на вимір стійкості ланцюгів постачання в умовах геополітичних шоків.

Таблиця 3

Дорожня карта кооперації для країн із перехідною економікою

Горизонт	Правове регулювання	Стандарти та інтероперабельність	Сертифікація/безпека	Кадри та інфраструктура	Міжнародна кооперація / ринки
0–6 міс.	«Біла книга» портованості й *exit*-клауз; інвентаризація *switching/egress charges*	GAP-аналіз ISO/IEC 27001/27701/27017/27018 та мапінг на NIST CSF 2.0	Пілот сертифікації EUCC-рівня для критичних ІКТ-продуктів	Програма підготовки *cloud/security* архітекторів у держ-секторі	Заява про приєднання до IAP (DFFT); дорожня карта двосторонніх модулів даних
6–18 міс.	Проєктний закон/постанова щодо портованості; типові договори з *exit*-вимогами	Референс-архітектури для мультихмарності; каталоги форматів/інтерфейсів	Секторні профілі вимог; підготовка до EUCS/еквівалентів	Пілотні «суверенні» регіони у гіперскейлерів; CSIRT-процедури	Угода про обмін індикаторами (ISAC-моделі) з партнерами; промопрограми *nearshore*-експорту
18–36 міс.	Повна імплементація норм портованості; заборона *egress*-плат за графіком	Оновлення мапінгів (ISO/IEC ↔ NIST CSF 2.0); аудит інтероперабельності	Регулярний аудит і сертифікація провайдерів; взаємне визнання	Центри компетенцій (R&D + *security operations*); резервування/edge	Участь у спільних платформах даних; вихід на ринки з «міткою довіри»

Джерело: розроблено авторами на основі [4; 6]

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Cyber Europe exercises. *ENISA* : веб-сайт. URL: https://www.enisa.europa.eu/topics/cybersecurity-exercises/cyber-europe-programme (дата звернення: 24.08.2025)
2. EU Cybersecurity Certification – overview. *ENISA* : веб-сайт. URL: https://certification.enisa.europa.eu/index_en (дата звернення: 24.08.2025).
3. Global Trade Outlook and Statistics – April 2024. *WTO* : веб-сайт. URL: https://www.wto.org/english/res_e/publications_e/trade_outlook24_e.htm (дата звернення: 24.08.2025)
4. Guo S., Li X. Cross-border data flow in China: Shifting from restriction to relaxation? *Computer Law & Security Review*. 2025. Vol. 56, Article 106079. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 4806703
5. Gupta S., Ghosh P., Sridhar V. Impact of data trade restrictions on IT services export: A cross-country analysis. *Telecommunications Policy*. 2022. Vol. 46, Iss. 9, Article 102403. DOI: https://doi.org/10.1016/j.telpol. 2022.102403
6. Herman P. R., Oliver S. Trade, policy, and economic development in the digital economy. *Journal of Development Economics*. 2023. Vol. 164, Article 103135. DOI: https://doi.org/10.1016/j.jdeveco.2023.103135
7. Honcharenko V., Panteleimonenko A., Pozhar A., Stetsenko V. Cooperatives in IT sector: theoretical and practical aspects. *Periodicals of Engineering and Natural Sciences*. 2019. Vol. 7(2), pp. 597–607. DOI: https://doi.org/10.21533/pen.v10.i1.570
8. Li H., Han J., Xu Y. The effect of the digital economy on services exports competitiveness and ternary margins. *Telecommunications Policy*. 2023. Vol. 47, Iss. 7, Article 102596. DOI: https://doi.org/10.1016/j.telpol.2023.102596
9. Zhang Y., Xu J., Yang W. Analysis of the evolution characteristics of international ICT services trade based on complex network. *Telecommunications Policy*. 2024. Vol. 48, Iss. 3, Article 102697. DOI: https://doi.org/10.1016/j.telpol.2023.102697
10. Гончаренко В. В. Про зміни концепції розвитку системи кредитної кооперації та її можливий вплив на кредитно-кооперативний сектор національної економіки. *Науковий вісник ПУЕТ: Економічні науки*. 2011. № 5(50), С. 99–107. URL: http://dspace.puet.edu.ua/bitstream/123456789/3301/1/ 2012-Gonch-3.pdf
11. Гончаренко В. В. Кооператив-особлива форма кооперації та неприбуткової господарської діяльності. Основи сільськогосподарської обслуговуючої кооперації. Навчальний посібник. За ред. В. В. Зіновчука. Київ : «Вища освіта», 2001, С. 183–199 URL: http://dspace.puet.edu.ua/bitstream/123456789/3292/1/2001-Gonch-Pantel-1.pdf

REFERENCES:

1. Cyber Europe exercises. ENISA. Available at: https://www.enisa.europa.eu/topics/cybersecurity-exercises/cyber-europe-programme (accessed August 24, 2025)
2. EU Cybersecurity Certification – overview. ENISA. Available at: https://certification.enisa.europa.eu/index_en (accessed August 24, 2025)
3. Global Trade Outlook and Statistics – April 2024. WTO. Available at: https://www.wto.org/english/res_e/publications_e/trade_outlook24_e.htm (accessed August 24, 2025)
4. Guo S., Li X. (2025) Cross-border data flow in China: Shifting from restriction to relaxation? *Computer Law & Security Review*, Vol. 56. Article 106079. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806703
5. 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
6. 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
7. 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
8. 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
9. 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
10. Honcharenko V. V. Pro zminy kontseptsiyi rozvytku systemy kredytnoyi kooperatsiyi ta yiyi mozhlyvyy vplyv na kredytno-kooperatyvnyy sektor natsional'noyi ekonomiky [On changes in the concept of the development of the credit cooperative system and its possible impact on the credit cooperative sector of the national economy]. Naukovyy visnyk PUET: *Ekonomichni nauky – Scientific Bulletin of PUET: Economic Sciences.* 2011. # 5(50), pp. 99–107. Available at: http://dspace.puet.edu.ua/bitstream/123456789/3301/1/ 2012-Gonch-3.pdf

11. Honcharenko V. V. Kooperatyv – osoblyva forma kooperatsiyi ta neprybutkovoyi hospodars'koyi diyal'nosti [Cooperative – a special form of cooperation and non-profit economic activity]. *Osnovy sil's'kohospodars'koyi obsluhovuyuchoyi kooperatsiyi – Fundamentals of agricultural service cooperation*. Textbook. Edited by V. V. Zinovchuk. Kyiv : “Vyshcha osvita”, 2001, pp. 183–199 Available at: http://dspace.puet.edu.ua/bitstream/123456789/3292/1/2001-Gonch-Pantel-1.pdf