



Цифровий декаплінг як інструмент геоекономічної конкуренції: виклики та можливості для забезпечення цифрового суверенітету

Яковенко Ярослава Юріївна,

доктор філософії, доцент кафедри економіки, Кременчуцький
національний університет імені Михайла Остроградського,
м. Кременчук, Україна, <https://orcid.org/0000-0001-5042-2701>

Прийнято: 18.08.2025 | Опубліковано: 31.08.2025

***Анотація.** Глобальна боротьба за реалізацію цифрового суверенітету стала головним каталізатором цифрового декаплінгу — процесу технологічного та економічного розмежування, що керується логікою геополітики та національної безпеки, а не принципами економічної інтеграції.*

У статті доведено, що цифровий декаплінг є наслідком фундаментальної несумісності трьох провідних моделей цифрового управління: американської (ринково-орієнтованої), китайської (державно-центричної) та європейської (регуляторно-керованої). Детально проаналізовано стратегії та ключові політичні інструменти кожної з моделей: техно-націоналізм США, що реалізується через експортний контроль та субсидії (CHIPS Act); державно-керований підхід Китаю, спрямований на технологічну самодостатність («Made in China 2025»); та регуляторна сила ЄС («ефект Брюсселя»), що базується на екстериторіальному законодавстві (GDPR, AI Act). Розглянуто також альтернативні стратегії, зокрема індійську модель цифрової публічної



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

інфраструктури (India Stack) та «техно-демократичне балансування» Південної Кореї.

Цифровий декаплінг трансформує глобальний цифровий простір, посилюючи його фрагментацію (Сплінтернет) та перетворюючи технології на головну арену геополітичного суперництва. Для держав, подібних до України, це створює складну дилему між необхідністю залучення іноземних технологій для забезпечення стійкості та ризиком втрати стратегічної автономії у майбутньому.

Окрему увагу приділено аналізу наслідків цифрового декаплінгу для України, зокрема у контексті поняття «цифрового ленд-лізу» — безпрецедентної технологічної підтримки з боку міжнародних партнерів, яка забезпечила цифрову стійкість країни в умовах повномасштабного вторгнення. Водночас виявлено стратегічний парадокс: рятуючи Україну сьогодні, «цифровий ленд-ліз» формує довгострокову залежність її критичної інфраструктури від іноземних технологічних платформ, що створює значні ризики для майбутнього цифрового суверенітету держави.

Ключові слова: *цифровий суверенітет, цифровий декаплінг, геоекономіка, техно-націоналізм, цифрова стійкість, цифрова інфраструктура.*

Digital Decoupling as an Instrument of Geoeconomic Competition: Challenges and Opportunities for Ensuring Digital Sovereignty

Yaroslava Yakovenko,

PhD, Associate Professor of the Department of Economics, Kremenichuk Mykhailo Ostrohradskyi National University, Kremenichuk, Ukraine,

<https://orcid.org/0000-0001-5042-2701>



Abstract. *The global struggle for digital sovereignty has become the main catalyst for digital decoupling, a process of technological and economic decoupling driven by the logic of geopolitics and national security rather than by the principles of economic integration.*

The paper argues that digital decoupling is a consequence of the fundamental incompatibility of three leading models of digital governance: the American (market-oriented), the Chinese (state-centric), and the European (regulatory-driven). The strategies and key policy instruments of each model are analyzed in detail: the US techno-nationalism implemented through export controls and subsidies (CHIPS Act); China's state-driven approach aimed at technological self-sufficiency ("Made in China 2025"); and the EU's regulatory power ("Brussels effect") based on extraterritorial legislation (GDPR, AI Act). Alternative strategies are also considered, including the Indian model of digital public infrastructure (India Stack) and South Korea's "techno-democratic balancing".

Digital decoupling transforms the global digital space, increasing its fragmentation (Splinternet) and turning technology into the main arena of geopolitical rivalry. For states like Ukraine, this creates a difficult dilemma between the need to attract foreign technologies to ensure sustainability and the risk of losing strategic autonomy in the future.

Special attention is paid to the analysis of the consequences of digital decoupling for Ukraine, in particular in the context of the concept of "digital lend-lease" — unprecedented technological support from international partners, which ensured the country's digital resilience in the face of a full-scale invasion. At the same time, a strategic paradox is revealed: while saving Ukraine today, "digital lend-lease" forms a long-term dependence of its critical infrastructure on foreign technological platforms, which creates significant risks for the future digital sovereignty of the state.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Keywords: *digital sovereignty, digital decoupling, geoeconomics, technological nationalism, digital resilience, digital infrastructure.*

Постановка проблеми. Класична концепція державного суверенітету, що історично сформувалася після підписання Вестфальського миру у 1648 році, базувалася на принципах територіальності, верховенства влади в межах чітко визначених кордонів та невтручання у внутрішні справи інших держав [1]. Протягом століть Вестфальська модель слугувала основою міжнародних відносин, однак процеси глобалізації, зростання впливу транснаціональних корпорацій та, найголовніше, поява глобальної мережі Інтернет та пов'язаних з нею цифрових технологій, які за своєю природою є транскордонними, децентралізованими та значною мірою непідконтрольними окремим урядам, спричинили необхідність пошуку нових підходів [2]. Так, виникла концепція цифрового суверенітету, що позначає право та правоспроможність держави контролювати власну цифрову інфраструктуру, дані, що генеруються, та технологічні стандарти [3]. Прагнення до цифрового суверенітету, тобто контролю над даними та інфраструктурою, часто призводить до активізації політик декаплінгу. І хоча воно зрозуміле з точки зору безпеки, створює напругу між національним контролем та глобальною взаємозалежністю, що може мати як непередбачені позитивні, так і значні негативні наслідки. Водночас, попри значну увагу до теоретичного осмислення мотивів, що спонукають держави до боротьби за цифровий суверенітет, недостатньо дослідженням залишається сам інструментарій цієї боротьби.

Аналіз останніх досліджень і публікацій свідчить, що ідея цифрового суверенітету, яка ще десятиліття тому асоціювалася переважно з авторитарними режимами [4], що прагнули контролювати інформаційні потоки, сьогодні стала лейтмотивом цифрової політики багатьох демократичних країн, зокрема Європейського Союзу. Крім того, це ще і про



просуння європейських цінностей, захист права громадян на приватність та зменшення стратегічної залежності від техногігантів [5]. Для інтерпретації таких підходів дослідники звертаються до теоретичного інструментарію економіки і міжнародних економічних відносин. Так, з позицій неореалізму, кіберпростір розглядається як нова арена для боротьби за владу та безпеку між державами. Тобто, у цьому контексті технологічна перевага стає ключовим компонентом національної могутності, а кібератаки та кібершпигунство – новими інструментами реалізації національних інтересів [6]. Держави прагнуть максимізувати свою кіберпотужність для захисту власних інтересів та отримання переваг над конкурентами, що неминуче веде до дилеми безпеки, коли оборонні заходи однієї держави сприймаються іншими як загроза.

На противагу цьому, конструктивістський підхід пропонує розглядати «цифровий суверенітет» не як об'єктивну реальність, а як соціальний конструкт [7], тобто значення цього поняття є плинним і залежить від контексту, цінностей та владних відносин, в яких воно артикулюється [8]. Таким чином, боротьба за визначення змісту цифрового суверенітету є, по суті, боротьбою за контроль над майбутнім цифрового світу.

Виділення невирішених раніше частин загальної проблеми. Нині бракує комплексного аналізу суперечливого впливу політик декаплінгу, які, з одного боку, спрямовані на зміцнення національної безпеки та суверенітету, а з іншого — створюють значні економічні витрати, ризики фрагментації глобального цифрового простору та нові стратегічні вразливості.

Мета статті – аналіз цифрового декаплінгу як ключового інструменту сучасної геоекономічної конкуренції та оцінка його суперечливого впливу на процеси забезпечення цифрового суверенітету держав. Для досягнення мети використано інструментарій теорій міжнародних відносин, зокрема неореалізму та конструктивізму, а також застосовано метод порівняльного аналізу для дослідження глобальних моделей цифрового управління.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Виклад основного матеріалу дослідження. Наслідком глобальної боротьби за цифровий суверенітет і став цифровий декаплінг. На відміну від традиційної економічної логіки глобалізації, що прагнула до інтеграції та оптимізації глобальних ланцюгів вартості, декаплінг керується логікою геополітики та національної безпеки. Загалом можна виділити три моделі цифрового управління на макrorівні, фундаментальна несумісність яких тільки поглиблює цифровий декаплінг: американська (ринковоорієнтована та капіталоцентрична), китайська (державоцентрична з фокусом на суверенітет) та європейська (регфляторно-керована та правозахисна). Розбіжності в основних фокусах кожної моделі (рис.1) призводять не тільки до різних управлінських підходів, а й регуляторних рамок та технологічних стандартів – кожен кут умовного «трикутника» формує власний цифровий простір, виходячи з закладених цінностей, що ускладнює глобальну співпрацю та взаємодію.

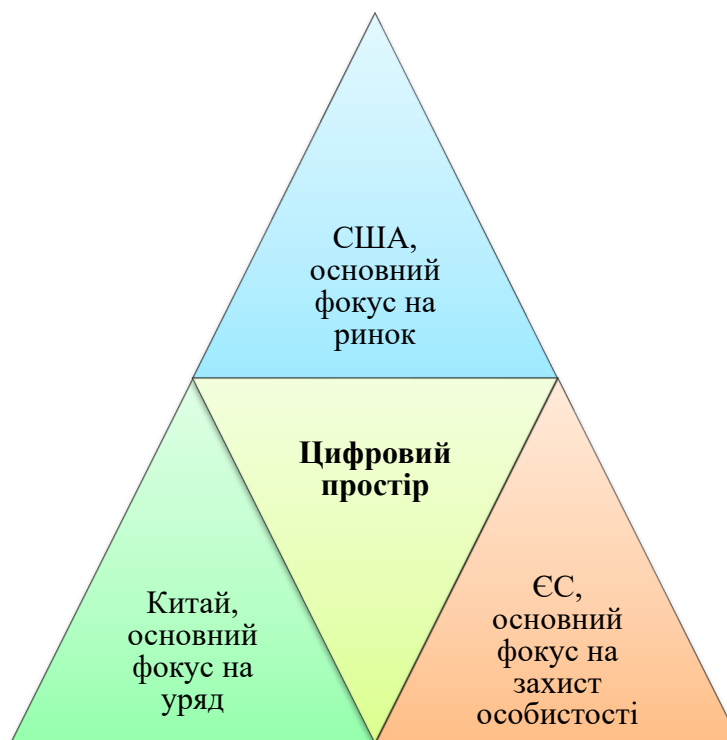


Рис 1. Трикутник геополітики цифрового простору

Джерело: узагальнено автором на основі [9-11, 21]



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Американська модель пріоритезує ринкові інтереси, історично будучи сформованою на засадах *laissez-faire*, економічної доктрини, яка виступала за мінімальне чи повністю відсутнє втручання держави в економіку. Особливо відчутним вплив на політику США цього підходу став у період «позолоченої епохи», тобто часи відродження ідей вільного ринку у 1980-х роках. Попри те, що сама доктрина не являє собою причину цифрового декаплінгу, відсутність координації та регулювання якраз створює передумови для розбіжностей у підходах до цифрового управління.

Крім того, саме підхід *laissez-faire* посприяв безперешкодному зростанню технологічних компаній-лідерів і сприяв тому, що вільний обмін інформацією став інструментом просування демократичних цінностей і американських бізнес-інтересів [12, 13]. Разом з тим, в сучасних умовах цей підхід зазнає змін – США переходять до децентралізованого, подекуди галузевого (наприклад, у Федеральній торговій комісії чи Національному управлінні безпеки руху на трасах) стилю регулювання, унормовуючи використання ІІТ у цих сферах [14]. Стратегія США є дуалістичною і поєднує "наступальні" та "захисні" заходи. Її головна мета – збереження технологічного лідерства та стримування Китаю як головного геополітичного суперника. "Захисні" заходи включають широкий арсенал інструментів: експортний контроль над чутливими технологіями (напівпровідники, обладнання для їх виробництва); скринінг іноземних інвестицій; санкції та візові обмеження. "Наступальні" заходи спрямовані на зміцнення власної інноваційної та виробничої бази, найяскравішим прикладом чого є CHIPS and Science Act, що передбачає багатомільярдні субсидії для будівництва заводів з виробництва напівпровідників на території США.

Китайська модель, на відміну від американської, – державноцентрична. Тобто, пріоритет надається державі, її суверенітету та соціальній стабільності [15]. Фактично ця модель першочергово орієнтована на посилення влади та



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

уряду, а вже потім – на відповідність цифрової економіки політиці та ідеології правлячої партії.

Звісно, регуляторна політика Китаю проявляється і в нормативному, і в практичному аспектах – від державного нагляду та превалювання інтересів держави і національно, прописаних у Законі про захист персональної інформації [16], до «Великого китайського файрволу», який контролює глобальний Інтернет-трафік [17].

Пріоритетність інтересів держави прослідковується і в політиці регулювання ІІІ в Китаї, коли проводиться аудит попередньо зареєстрованих алгоритмів на їх відповідність державним цінностям [18].

Стратегія Китаю є державно-центричною і розглядає технологічний розвиток як інструмент для досягнення цілої низки цілей: економічної модернізації, посилення соціального контролю та проектування глобального впливу. Ключовими ініціативами є «Made in China 2025», спрямована на досягнення самодостатності у 10 ключових високотехнологічних секторах, а також «Цифровий шовковий шлях», що просуває китайські технологічні стандарти та інфраструктурні проекти в країнах, що розвиваються.

Німеччина та Індія вже розробляють власні стратегії щодо декаплінгу з Китаєм, які відрізняються залежно від їхніх двосторонніх відносин та внутрішніх обставин [19]: Індія ввела значні обмеження на ринковий доступ для китайського обладнання та програмного забезпечення, а Німеччина демонструє меншу схильність до повного декаплінгу, зберігаючи економічну співпрацю в певних секторах.

Європейська модель демонструє третій, зовсім інакший підхід, коли першочерговою задачею є захист особистості та її фундаментальних прав. На законодавчому рівні ці принципи закладено у Загальному регламенті про захист даних (GDPR) та Законі про штучний інтелект (AI Act), всеосяжних та екстериторіальних. Крім того, транснаціональні компанії, щоб мати доступ до



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

ринку ЄС, приймають ці стандарти за основу, беручи на себе зобов'язання щодо оцінки впливу на фундаментальні права користувачів з метою їх захисту [92]. Так, для прикладу, Закон про штучний інтелект запроваджує чотирирівневу структуру для категоризації ризиків (неприйнятний, високий, лімітований, мінімальний) [20].

Стратегія Європейського Союзу формулюється через концепцію «відкритої стратегічної автономії» (англ. open strategic autonomy), коли оловним інструментом ЄС є регуляторна влада та стандартизація. Паралельно ЄС ініціює проекти зі створення власної технологічної інфраструктури (наприклад, GAIA-X – ініціатива з побудови федеративної та суверенної хмарної інфраструктури, що має на меті запропонувати альтернативу американським (Amazon Web Services, Microsoft Azure, Google Cloud) та китайським компаніям).

У цьому контексті варто зазначити, що відставання в інноваціях у цифровій сфері і зумовило той факт, що європейська модель нині являє собою форму стратегічної автономії. Відповідно, посилений регуляторний контроль ЄС стає геополітичним інструментом на протипагу монополістичним американській та китайській моделям, що важливо з точки зору розвитку світової торгівлі та балансу сил на міжнародній арені.

Разом з тим, фундаментальна несумісність моделей між собою, особливо в розрізі питань регулювання транскордонних потоків даних, і їх постійне протистояння між собою і слугують тим механізмом, що уможливорює цифровий декаплінг у глобальному масштабі (табл. 1).



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Таблиця 1

Порівняльний аналіз глобальних моделей цифрового управління

Параметр моделі	Американська	Європейська	Китайська
Основна спрямованість	Ринково-орієнтована, пріоритет інновацій та свободи слова	Правозахисна, пріоритет фундаментальних прав особистості	Державно-центрична, пріоритет державного суверенітету та соціальної стабільності
Головний бенефіціар	Технологічні компанії, ринок	Громадяни, споживачі	Держава, Комуністична партія
Ключове законодавство	CLOUD Act, секторальні норми	GDPR, AI Act, Digital Services Act (DSA), Digital Markets Act (DMA)	Cybersecurity Law (CSL), Data Security Law (DSL), Personal Information Protection Law (PIPL)
Підхід до потоків даних	Сприяння вільному потоку даних, але з правом доступу уряду для правоохоронних цілей (CLOUD Act)	Вільний потік даних у межах ЄСП; суворі вимоги до передачі за межі ЄС для захисту прав	Жорсткі вимоги до локалізації даних, державний контроль над транскордонними передачами, особливо для критичної інфраструктури
Регулювання ІІІ	Децентралізований, галузевий, добровільні стандарти, акцент на інноваціях	Комплексний, горизонтальний, заснований на ризиках (4 рівні), з жорсткими вимогами до систем високого ризику	Вертикальний, державний контроль, обов'язкова реєстрація та аудит алгоритмів на відповідність державним цінностям
Модель правозастосування	Різні федеральні агентства та законодавство штатів	Наднаціональні інституції ЄС та національні наглядові органи в кожній країні-члені	Централізований контроль з боку державних органів, зокрема Адміністрації кіберпростору Китаю (CAC)

Джерело: складено автором на основі [11, 16-18, 20]

Як бачимо, в геополітичному вимірі декаплінг стає інструментом конфронтації та управління ризиками. Його метою є не стільки сукупний



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

економічний вигравш, скільки мінімізація стратегічних вразливостей та досягнення переваги у відносному, а не абсолютному вимірі. Порівняльний аналіз стратегій цифрового суверенітету (табл. 2) демонструє, що логіка декаплінгу визначається не законами ринку, а законами геополітичного суперництва.

Таблиця 2

Порівняльний аналіз стратегій цифрового суверенітету США, ЄС та Китаю

Критерій порівняння	Сполучені Штати Америки	Європейський Союз	Китай
Ключова ідея	Техно-націоналізм, орієнтований на національну безпеку та збереження глобального ринкового і технологічного лідерства	«Відкрита стратегічна автономія», заснована на цінностях (права людини, приватність, демократія) та регуляторній силі	Державно-керований техно-націоналізм, спрямований на економічний розвиток, соціальний контроль та посилення глобального впливу
Основні політичні ініціативи	CHIPS and Science Act, National Defense Authorization Act (NDAA), Inflation Reduction Act (IRA)	General Data Protection Regulation (GDPR), Digital Services Act (DSA), AI Act, European Chips Act, ініціатива GAIA-X	«Made in China 2025», «Digital Silk Road», Personal Information Protection Law (PIPL), політика злиття цивільних та військових технологій
Основні інструменти реалізації	Експортний контроль (Entity List), санкції, скринінг інвестицій (CFIUS), тарифи, субсидії для вітчизняного виробництва	Екстериторіальне регулювання ("ефект Брюсселя"), стандартизація, створення федеративної інфраструктури, антимонопольні розслідування	Державні субсидії та інвестиції, вимоги до локалізації даних, кібершпигунство, примусова передача технологій, контроль над стандартами

Джерело: складено автором на основі [6, 22-23, 33]

Крім того, варто відзначити, що цифровий декаплінг посилюється процесами фрагментації, які отримали прояв у вигляді кібербалканізації та Сплінтернету (англ. Splinternet). Перший термін використовується для позначення неможливості функціонування єдиного, відкритого та глобального кіберпростору [24], а другий – для характеристики розколу Інтернету на



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

окремі регіональні чи національні блоки [25]. Технологічний декаплінг, що просувається США та Китаєм, може стати шляхом реалізації обох згаданих явищ, адже їх драйвером стала тривала хвиля мілітаризації кіберпростору, що проявляється в намаганні окремих держав створити ізольовані мережі (наприклад, згаданий раніше китайський файрвол чи російський рунет) з метою ідеологічного та політичного контролю інформаційного простору та відбувається одночасно на кількох рівнях (фізичному – центри обробки даних, підводні кабелі; логічному – протоколи, доменні системи; семантичному – контент, додатки). Популярна раніше ідея, що інтернет та цифрові технології сприяють глобальній інтеграції, сьогодні не сприймається як абсолют, оскільки існує також концепція цифрової залізної завіси, коли уряди намагаються підтримувати технологічну перевагу шляхом обмежень, що, парадоксально, може прискорювати інновації в обхід цих обмежень [26]. Очевидно, це свідчить про зміну напрямку досліджень від оптимістичних поглядів на глобалізацію до занепокоєння щодо фрагментації та її наслідків для демократії, вільних ринків та міжнародної співпраці.

Разом з тим, спостерігаються прояви «символічного декаплінгу», коли ТНК розробляють стратегії гнучких архітектур (англ. flexible architecture) чи вдаються до крайніх форм інституційного декаплінгу (наприклад, «в Китаї для Китаю») з метою входження на певний ринок і задля можливості одночасно підпорядковуватися різним моделям цифрового управління, дотримуючись суперечливих вимог [27]. Це неминуче веде до зниження ефективності, зростання собівартості продукції, що перекладається на споживачів у вигляді вищих цін, та, як показують економічні моделі, до сукупних втрат глобального добробуту.

Цікавим є досвід Індії, яка демонструє принципово інший підхід до цифрового суверенітету, який базується не на регулюванні чи промислових субсидіях, а на створенні цифрової публічної інфраструктури (англ. Digital



Public Infrastructure, DPI). Ця модель, відома як India Stack, являє собою набір відкритих програмних інтерфейсів (API) та цифрових суспільних благ, що надаються державою як відкрита платформа, на базі якої приватний сектор може створювати інноваційні послуги [28]. Економічний та соціальний вплив індійської моделі заслуговує на увагу, адже вона сприяла якісному поступу у фінансовій інклюзії, значно знизила транзакційні витрати для бізнесу та громадян, а також створила динамічну екосистему для фінтех-стартапів, які будують свої продукти на базі державної інфраструктури та активно просувається Індією як приклад для країн Глобального Півдня.

Південна Корея, будучи одним зі світових технологічних лідерів, особливо у виробництві напівпровідників, та водночас перебуваючи у складному геополітичному становищі між своїм головним союзником США та найбільшим торговельним партнером Китаєм, реалізує стратегію, яку можна охарактеризувати як «техно-демократичне балансування» [29]. Стратегія Сеула базується на таких засадах: 1) використання технологічної переваги як стратегічного активу; 2) активна державна промислова політика; 3) стратегічна диверсифікація та багатовекторна дипломатія.

Щодо останнього, то намагаючись уникнути надмірної залежності від одного партнера, Південна Корея, поглиблюючи військово-технологічний альянс із США, одночасно активно розвиває співпрацю з іншими центрами сили. Було укладено Цифрове партнерство з ЄС, що охоплює співпрацю в галузі ШІ, управління даними та кібербезпеки. Сеул також бере активну участь у багатосторонніх форматах, таких як Індो-Тихоокеанська економічна рамка (IPEF), для просування своїх інтересів у сферах цифрової торгівлі та стандартів. Проте ця стратегія балансування пов'язана зі значними ризиками та непередбачуваними наслідками [30]: 1) вразливість до американських санкцій; 2) ризик втрати китайського ринку; 3) конкуренція та «відтік мізків», що створює пряму загрозу технологічному лідерству Південної Кореї.



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

Яскравим прикладом відмінностей у підходах до цифрового суверенітету є регулювання штучного інтелекту, адже механізми суттєво відрізняються. Так, EU AI Act є втіленням європейського регуляторного підходу. Він базується на жорсткій, ризик-орієнтованій класифікації, а South Korea's AI Basic Act, навпаки, є прикладом інноваційно-орієнтованого підходу. Він також використовує ризик-орієнтовану логіку, але є значно гнучкішим і спрямованим на баланс між регулюванням та стимулюванням розвитку. Обидва підходи ілюструють фундаментальну дилему в сучасному технологічному регулюванні: як забезпечити безпеку та захист прав, не придушивши при цьому інновації та економічне зростання.

Що стосується цифрового суверенітету нашої країни, то Україна продемонструвала феноменальну цифрову стійкість в умовах повномасштабного вторгнення РФ та постійних кібератак ворога, які мають на меті не лише шпигунство, а й руйнування критичної інфраструктури, дестабілізацію державних інституцій та поширення паніки серед населення. Найбільш вразливими виявилися енергетичний сектор, державні реєстри, фінансові установи та телекомунікаційні мережі.

Стійкість України значною мірою стала можливою завдяки безпрецедентній технологічній підтримці з боку міжнародних партнерів. Цю допомогу можна охарактеризувати за аналогією з історичним ленд-лізом часів Другої світової війни як «цифровий ленд-ліз» [31], тобто надання Україні на пільгових або безоплатних умовах критично важливих технологій, хмарних сервісів, програмного забезпечення, обладнання та експертизи для підтримки обороноздатності та функціонування держави.

Однак, попри свою життєву необхідність, «цифровий ленд-ліз» створює фундаментальний стратегічний парадокс. Рятуючи Україну сьогодні, він водночас формує глибоку та довгострокову залежність її критичної інфраструктури – державної, військової, енергетичної – від іноземних,



ЗДОБУТКИ ЕКОНОМІКИ: ПЕРСПЕКТИВИ ТА ІННОВАЦІЇ

переважно американських, технологічних платформ та корпорацій [32]. Подібна залежність несе в собі значні ризики для майбутнього цифрового суверенітету України: вразливість до змін у ціновій політиці корпорацій, залежність від політичної волі країн-партнерів (що особливо гостро відчувається в контексті змін у політичному керівництві США), ризики, пов'язані з безпекою даних, що зберігаються за кордоном, та потенційні вразливості в самих іноземних системах.

Висновки. Проведене дослідження дозволяє зробити висновок, що логіка геополітичного суперництва та національної безпеки переважає над принципами економічної глобалізації. Центральним інструментом і водночас наслідком цієї трансформації став цифровий декаплінг — процес свідомого технологічного та інфраструктурного розмежування між провідними світовими державами, що веде до фрагментації раніше єдиного цифрового простору. Для України та інших держав, що перебувають на перетині геополітичних розломів, здатність виробити довгострокову стратегію управління технологічними залежностями та розбудови власної інноваційної екосистеми стає одним із ключових елементів забезпечення національної безпеки та виживання у XXI столітті.

Список використаних джерел

1. State Sovereignty in International Relations. Issuu. URL: https://issuu.com/marcbatko/docs/state_20sovereignty_20in_20international_20relati (дата звернення: 27.06.2025).
2. A Critical Reflection on Sovereignty in International Relations Today. E-International Relations. URL: <https://www.e-ir.info/2019/02/09/a-critical-reflection-on-sovereignty-in-international-relations-today/> (дата звернення: 27.06.2025).



3. Цифровий суверенітет як необхідність. Indevlab. URL: <https://indevlab.com/uk/blog-ua/tsifrovij-suverenitet-yak-neobhidnist/> (дата звернення: 27.06.2025).
4. Гвоздьова О. В., Тимохін В. В. Забезпечення цифрового суверенітету держави в умовах індустрії 4.0. Харків : Харківський національний університет радіоелектроніки, 2022. URL: <https://openarchive.nure.ua/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/download> (дата звернення: 27.06.2025).
5. Цифровий суверенітет Європейського Союзу та перспективи України. Центр оборонних стратегій. URL: <https://csd.org.ua/2020/11/17/czyfrovuj-suverenitet-yevropejskogo-soyuzu-ta-perspektyvy-ukrayiny/> (дата звернення: 27.06.2025).
6. Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. URL: https://www.researchgate.net/publication/375428807_Neorealist_Analysis_of_Security_Dilemma_in_Cyberspace_A_Quantitative_Study (дата звернення: 27.06.2025).
7. Kipker D.-K., Tzanetatos D., Malgieri G. Attributes of Digital Sovereignty: A Conceptual Framework // International Affairs. 2025. Vol. 101, Issue 4. P. 1461–1478. URL: <https://www.tandfonline.com/doi/full/10.1080/14650045.2025.2521548?src=exp-la> (дата звернення: 27.06.2025).
8. Suri A. R. Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy // Global: Jurnal Politik Internasional. 2024. Vol. 26, no. 1. P. 1–28. URL: <https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1065&context=global> (дата звернення: 27.06.2025).



9. Kastner A., Rolland N. The Global Digital Governance Map. New America. URL: <https://www.newamerica.org/planetary-politics/reports/governing-the-digital-future/the-global-digital-governance-map/> (дата звернення: 27.06.2025).
10. Global approaches to digital sovereignty: Competing definitions and contrasting policy. ECDPM. URL: <https://ecdpm.org/work/global-approaches-digital-sovereignty-competing-definitions-and-contrasting-policy> (дата звернення: 27.06.2025).
11. Tritto A. 'Digital Empires': The China-EU-US Competition Over Tech Regulations // The Diplomat. URL: <https://thediplomat.com/2023/10/digital-empires-the-china-eu-us-competition-over-tech-regulations/> (дата звернення: 27.06.2025).
12. Has the US Abdicated Global Digital Leadership? CEPA. URL: <https://cepa.org/article/has-the-us-abdicated-global-digital-leadership/> (дата звернення: 27.06.2025).
13. AI Governance Cheat Sheet: Comparing Regulatory Frameworks. Gradient Flow. URL: <https://gradientflow.com/ai-governance-global-cheat-sheet/> (дата звернення: 27.06.2025).
14. Data Sovereignty in the Age of Digital Nationalism: The Case of TikTok and the Global Fragmentation of the Internet // Student Journal of Information Privacy Law. URL: <https://sjipl.maine.law.maine.edu/2025/04/30/data-sovereignty-in-the-age-of-digital-nationalism-the-case-of-tiktok-and-the-global-fragmentation-of-the-internet/> (дата звернення: 27.06.2025).
15. Eichensehr K. E. Governing the digital economy: transatlantic accommodation and ... // International Journal. 2024. Vol. 79, Issue 2. URL: <https://www.tandfonline.com/doi/full/10.1080/07036337.2024.2398429> (дата звернення: 27.06.2025).



16. Baskaran V. How do the European Union's GDPR and China's PIPL regulate. URL: <https://ipr.blogs.ie.edu/2025/01/27/how-do-the-european-unions-gdpr-and-chinas-pipl-regulate-cross-border-data-flows/> (дата звернення: 27.06.2025).
17. Falk S., Schaffmann S. Rethinking EU Digital Policies: From Tech Sovereignty to Tech Citizenship. Carnegie Endowment for International Peace. URL: <https://carnegieendowment.org/research/2025/06/rethinking-eu-digital-policies-from-tech-sovereignty-to-tech-citizenship?lang=en> (дата звернення: 27.06.2025).
18. Comparative Analysis of AI Development Strategies: A Study of China's Ambitions and the EU's Regulatory Framework. EuroHub4Sino. URL: <https://eh4s.eu/publication/comparative-analysis-of-ai-development-strategies-a-study-of-chinas-ambitions-and-the-e-us-regulatory-framework> (дата звернення: 27.06.2025).
19. Digital Decoupling. Prism → Sustainability Directory. URL: <https://prism.sustainability-directory.com/term/digital-decoupling/> (дата звернення: 27.06.2025).
20. Prasso S. China PIPL vs GDPR: Key Differences to Know. Captain Compliance. URL: <https://captaincompliance.com/education/china-pipl-vs-gdpr/> (дата звернення: 27.06.2025).
21. Yakovenko, Y., & Shaptala, R. (2024). Study of digital twins as the driving force of digital transformation and achieving the goals of sustainable development. Technology Audit and Production Reserves, 2(4(76), 11–20. <https://doi.org/10.15587/2706-5448.2024.301423> (дата звернення: 27.06.2025).
22. Pahre R. Power, Conflict, and Technology: Delineating Empirical Theories in a Changing World // Oxford Research Encyclopedia of Politics. URL: <https://oxfordre.com/politics/display/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-587> (дата звернення: 27.06.2025).



23. The geopolitics of AI and the rise of digital sovereignty. Brookings Institution. URL: <https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/> (дата звернення: 27.06.2025).
24. Splinternet: how geopolitics is fracturing cyberspace. Polytechnique Insights. URL: <https://www.polytechnique-insights.com/en/columns/geopolitics/splinternet-when-geopolitics-fractures-cyberspace/> (дата звернення: 27.06.2025).
25. The difference between decoupling and de-risking. URL: <https://www.hinrichfoundation.com/research/article/trade-and-geopolitics/china-decoupling-vs-de-risking/> (дата звернення: 27.06.2025).
26. García-Herrero A. 30 years on: from the Iron Curtain to digital curtains. Real Instituto Elcano. URL: <https://www.realinstitutoelcano.org/en/commentaries/1989-30-years-on-from-the-iron-curtain-to-digital-curtains/> (дата звернення: 27.06.2025).
27. Decoupling Digital Actions and Narratives: The Role of Firm Status // Academy of Management Proceedings. 2024. Vol. 2024, No 1. URL: <https://journals.aom.org/doi/full/10.5465/AMPROC.2024.18951abstract> (дата звернення: 27.06.2025).
28. India Stack: India's Digital Public Infrastructure Revolution [Електронний ресурс]. Egon Zehnder. URL: <https://www.egonzehnder.com/industries/technology-communications/digital/insights/the-rise-of-the-india-stack-addressing-indias-digital-public-infrastructure-revolution> (дата звернення: 27.06.2025).
29. Park J. South Korea as a techno-democratic power: strategic positioning. Fondation pour la Recherche Stratégique. URL: <https://www.frstrategie.org/en/programs/korea-security-and-diplomacy-program/south-korea-techno-democratic-power-strategic-positioning-and-cooperation-european-union-2025> (дата звернення: 27.06.2025).



30. Three Questions to June Park: South Korea, the United States, and the Gulf-Semiconductors in the Development of AI [Електронний ресурс]. Institut Montaigne. URL: <https://www.institutmontaigne.org/en/expressions/three-questions-june-park-south-korea-united-states-and-gulf-semiconductors-development-ai> (дата звернення: 27.06.2025).
31. Цифровізація економіки як фактор стійкого розвитку держави на тлі масштабної воєнної агресії (український досвід). 2022. URL: https://www.researchgate.net/publication/366706754_CIFROVIZACIA_EKONOMIKI_AK_FAKTOR_STIJKOGO_ROZVITKU_DERZAVI_NA_TLI_MASSTABNOI_VOENNOI_AGRESII_UKRAINSKIJ_DOSVID (дата звернення: 27.06.2025).
32. Defending The Invisible: Ukraine's Fight For Digital Sovereignty. Forbes Luxembourg. URL: <https://www.forbes.lu/defending-the-invisible-ukraine-fight-for-digital-sovereignty/> (дата звернення: 27.06.2025).
33. Яковенко Я. Ю. Формування та реалізація стратегії стійкого розвитку промислових підприємств: дис. ... д-ра філос.: 051. Кременчук, 2020. 279 с.