

УДК 327.56:004.738
DOI: 10.60022/3(3)-6S

Кузь Олег Миколайович

доктор філософських наук, професор
завідувач кафедри міжнародних відносин і політичної філософії
Харківський національний економічний університет імені Семена Кузнеця, Україна

Kuz Oleh

Doctor of Philosophical Sciences, Professor
Head of the Department of International Relations and Political Philosophy
Simon Kuznets Kharkiv National University of Economics, Ukraine
ORCID: 0000-0003-1359-2466

Жеребятнікова Ірина Володимирівна

кандидат соціологічних наук
доцент кафедри міжнародних відносин і політичної філософії
Харківський національний економічний університет імені Семена Кузнеця, Україна

Zherebiatnikova Iryna

PhD in Sociological Science
Associate Professor of the Department of International Relations and Political Philosophy
Simon Kuznets Kharkiv National University of Economics, Ukraine
ORCID: 0000-0001-7908-6780

Коннова Ніна Олексіївна

кандидат філософських наук
доцент кафедри міжнародних відносин і політичної філософії
Харківський національний економічний університет імені Семена Кузнеця, Україна

Konnova Nina

PhD in Philosophical Science
Associate Professor of the Department of International Relations and Political Philosophy
Simon Kuznets Kharkiv National University of Economics, Ukraine
ORCID: 0000-0002-7096-7714

ПОЛІТИКА ЦИФРОВОГО СУВЕРЕНІТЕТУ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА НАЦІОНАЛЬНІ ТРАЄКТОРІЇ ВПРОВАДЖЕННЯ В КРАЇНАХ СХІДНОГО ПАРТНЕРСТВА

Анотація. У статті комплексно проаналізовано концептуальні засади формування політики цифрового суверенітету Європейського Союзу та визначено особливості її реалізації в країнах Східного партнерства в умовах інтенсивної цифрової трансформації, загострення технологічної конкуренції та зростання гібридних загроз. Розкрито еволюцію підходів ЄС до забезпечення стратегічної автономії в цифровій сфері, що ґрунтується на поєднанні економічних, правових і безпекових інструментів, спрямованих на контроль над даними, розвиток цифрової інфраструктури та формування спільного регуляторного простору. Проаналізовано інституційні механізми реалізації цифрової політики, зокрема регулювання цифрових платформ, захист персональних даних, кібербезпеку, цифрову ідентифікацію та управління даними як основні елементи сучасного цифрового врядування.

Особливу увагу приділено процесам адаптації європейських стандартів у країнах Східного партнерства, де нормативна конвергенція відбувається нерівномірно та залежить від інституційної спроможності, економічного розвитку й безпекового середовища. Визначено відмінності національних моделей цифрових реформ, що проявляються у швидкості гармонізації законодавства, розвитку електронного врядування та формуванні цифрової довіри. Обґрунтовано, що інтеграція до цифрового простору ЄС супроводжується низкою викликів, зокрема технологічною залежністю, кіберзагрозами та ресурсними обмеженнями. Доведено, що політика цифрового суверенітету ЄС сприяє зміцненню цифрової стійкості, розвитку інноваційної економіки та підвищенню прозорості державного управління, стаючи важливим чинником інтеграції держав регіону до європейської цифрової екосистеми.

Ключові слова: цифровий суверенітет, Європейський Союз, цифрова політика ЄС, Східне



партнерство, єдиний цифровий ринок, цифрова інтеграція, кібербезпека, управління даними, цифрова стійкість, цифрова трансформація, стратегічна автономія, міжнародна інформаційна безпека.

DIGITAL SOVEREIGNTY POLICY OF THE EUROPEAN UNION AND NATIONAL IMPLEMENTATION TRAJECTORIES IN THE EASTERN PARTNERSHIP COUNTRIES

Abstract. *The purpose of the article is to provide a theoretical substantiation of the essence of the European Union's digital sovereignty policy and to identify the specific features and patterns of its implementation in the Eastern Partnership countries, taking into account national institutional, legal, and technological trajectories of digital development. The article provides a comprehensive analysis of the conceptual foundations of the European Union's digital sovereignty policy and identifies the specific features of its implementation in the Eastern Partnership countries under conditions of rapid digital transformation, increasing technological competition, and growing hybrid threats. The evolution of EU approaches to ensuring strategic autonomy in the digital sphere is examined, highlighting the combination of economic, legal, and security instruments aimed at strengthening data control, developing digital infrastructure, and forming a common regulatory space. The institutional mechanisms of EU digital policy implementation are analyzed, including the regulation of digital platforms, personal data protection, cybersecurity, digital identification, and data governance as key elements of modern digital governance.*

Special attention is paid to the adaptation of European digital standards in Eastern Partnership countries, where regulatory convergence remains uneven and largely depends on institutional capacity, economic development, and the security environment. Differences in national models of digital reform are identified, particularly regarding the pace of legislative harmonization, the development of e-government, and the establishment of digital trust mechanisms. The study substantiates that integration into the EU digital space is accompanied by challenges such as technological dependence, cybersecurity risks, and limited resources for implementing complex regulatory standards. It is concluded that the EU's digital sovereignty policy contributes to strengthening digital resilience, fostering innovation-driven economic development, and enhancing transparency in public administration, serving as a key driver of the Eastern Partnership countries' integration into the European digital ecosystem.

Keywords: *digital sovereignty, European Union, EU digital policy, Eastern Partnership, Digital Single Market, digital integration, cybersecurity, data governance, digital resilience, digital transformation, strategic autonomy, international information security.*

Постановка проблеми. Стрімка цифровізація економіки й суспільства зумовила переосмислення державного суверенітету, у якому контроль над даними, цифровою інфраструктурою та технологіями набуває стратегічного значення. У відповідь Європейський Союз (далі – ЄС) формує політику цифрового суверенітету, спрямовану на зміцнення автономії цифрової екосистеми, захист даних, посилення кібербезпеки та розвиток конкурентного цифрового ринку. Поширення європейських цифрових стандартів істотно впливає на країни Східного партнерства, які адаптують власні політики відповідно до аспис ЄС, розглядаючи цифрову трансформацію як інструмент модернізації управління та інтеграції до спільного цифрового простору. Водночас процес імплементації характеризується асиметрією, зумовленою відмінностями в рівні інституційного розвитку, ресурсів і безпекового середовища. За умов геополітичної нестабільності та зростання кіберзагроз актуалізується потреба комплексного дослідження політики цифрового суверенітету ЄС і особливостей її впровадження в державах Східного партнерства для забезпечення їхньої цифрової стійкості та ефективної інтеграції.

Аналіз останніх досліджень і публікацій. Аналіз наукових досліджень, присвячених політиці цифрового суверенітету ЄС та імплементації його стандартів у країнах Східного партнерства, дає змогу визначити основні напрями розвитку наукової думки та наявні дослідницькі прогалини. Зокрема, інституційні засади цифрових ініціатив ЄС розкривають І. Голуб'як та Н. Голуб'як [1]. Практичну модель цифрової держави на прикладі Естонії аналізують М. Петришина та М. Балабан [2]. Безпековий вимір цифрового суверенітету окреслює Ю. Калюжна [3], а його концептуально-теоретичне підґрунтя формують Л. Флоріді (L. Floridi) [4] й К. Тан та співавтори (K. Tan et al.) [5]. Правові аспекти цифрових прав і їхнього регулювання розкривають А. Лабик і колеги [6; 7], О. Корват [10] та О. Солодка [11]. Автори формують теоретико-правове підґрунтя дослідження цифрового й інформаційного суверенітету, акцентуючи на необхідності поєднання державного контролю над інформаційними ресурсами із

забезпеченням демократичних стандартів і прав людини. Розвиток Єдиного цифрового ринку ЄС у контексті трансформації держав Східного партнерства, як зазначають О. Цебенко та співавтори (O. Tsebenko et al.) [8], є дієвим інструментом економічної модернізації та інституційного зближення. Розширює цей підхід С. Гнатюк, висвітлюючи геополітичний вимір цифрового суверенітету та конкуренцію глобальних центрів сили за технологічне лідерство [9]. Водночас безпековим аспектом доповнює науковий дискурс П. Лисянський, демонструючи роль інформаційних та гібридних впливів у цифровому середовищі [13; 14]. Соціально-правові наслідки цифрової трансформації, зокрема питання захисту прав людини та соціальної стійкості в умовах цифровізації, аналізують Н. Заяць і колеги (N. Zaiats et al.) [12] та Н. Хотинська (N. Khotynska) [15].

Попри значний науковий доробок, недостатньо дослідженими залишаються порівняльні моделі імплементації цифрових стандартів ЄС у державах Східного партнерства та їхній реальний вплив на формування цифрової стійкості, інституційної спроможності й безпекової адаптації держав регіону. Найвні розвідки зосереджуються переважно на нормативно-правових або геополітичних аспектах, тоді як комплексний міждисциплінарний аналіз взаємозв'язку між цифровою інтеграцією, регуляторною конвергенцією та підвищенням стійкості держав залишається фрагментарним. Внесок статті полягає в системному узагальненні економічних, правових і безпекових підходів до політики цифрового суверенітету ЄС, а також у визначенні основних викликів і можливостей адаптації європейських цифрових стандартів для держав Східного партнерства. Це дає змогу поглибити розуміння механізмів їхньої інтеграції до європейської цифрової екосистеми.

Метою статті є теоретичне обґрунтування сутності політики цифрового суверенітету ЄС та визначення особливостей і закономірностей її імплементації в країнах Східного партнерства з урахуванням національних інституційних, правових і технологічних траєкторій цифрового розвитку.

Для досягнення мети сформульовано такі завдання:

- 1) дослідити концептуальні засади формування політики цифрового суверенітету ЄС, її інституційні механізми та основні регуляторні інструменти;
- 2) дослідити специфіку адаптації європейських цифрових норм і стандартів у країнах Східного партнерства та визначити відмінності національних моделей їхнього впровадження;
- 3) проаналізувати основні виклики та перспективи політики цифрового суверенітету як інструменту забезпечення стійкості та інтеграції країн Східного партнерства до єдиного цифрового простору ЄС.

Виклад основного матеріалу. Четверта індустриальна революція та процеси цифрової трансформації є визначальними чинниками сучасного економічного, політичного й соціального розвитку. Вони не лише стимулюють інноваційні зміни, а й підвищують здатність суспільств і держав протистояти глобальним викликам. Високі темпи технологічного прогресу зумовлюють потребу в оперативній адаптації політичних суб'єктів до нових реалій для збереження конкурентних позицій на міжнародній арені [1, с. 93].

У сучасних умовах глобального цифрового суперництва за домінування у сфері інформації та технологій провідними центрами впливу є Сполучені Штати Америки, Китай і ЄС, кожен із яких вибудовує власну модель цифрового суверенітету, зокрема шляхом модернізації нормативно-правового регулювання у сферах кібербезпеки, управління даними та цифрових прав. Якщо авторитарні політичні системи акцентують на посиленні централізованого контролю над інформаційними потоками та їхнього моніторингу, то демократичні держави змушені розв'язувати складніше завдання: забезпечувати рівновагу між потребами національної безпеки, стимулюванням інноваційного розвитку та гарантуванням фундаментальних прав і свобод людини [2, с. 6].

Комплексний характер сучасних гібридних загроз, які поєднують економічну залежність від зовнішніх цифрових платформ і військово-політичне протистояння в кіберпросторі, зумовив перегляд підходів ЄС до збереження власної безпеки. Поступово ЄС відмовився від ситуативних і розрізнених політичних рішень на користь формування цілісної та системної стратегії зміцнення цифрового суверенітету. Водночас його інституції стали визначальним чинником координації спільних зусиль, спрямованих на розроблення комплексної законодавчої бази, що враховує як значний потенціал цифрової трансформації, так і пов'язані з нею ризики [3, с. 1103].

Хоча концепція цифрового суверенітету все ще перебуває на стадії формування, практичні прояви її реалізації вже простежуються в нормативно-правових актах та політичних рішеннях різних держав. Так, у 2020 році державний секретар США М. Помпео заявив про намір американського уряду обмежити діяльність соціальної мережі «TikTok», обґрунтовуючи це потенційними загрозами національній безпеці. З огляду на значну популярність платформи, експерти наголошували на ризиках можливого збирання Китаєм персональних даних громадян США та застосування цифрових інструментів для впливу на громадську думку. Згодом відповідні обмежувальні заходи були офіційно

закріплені Актом про захист американців від застосунків, контрольованих іноземними противниками, який набрав чинності 19 січня 2025 року [4, с. 370].

Стрімкий розвиток інтернет-технологій, упровадження мереж п'ятого покоління та прогрес у сфері штучного інтелекту (далі – ШІ) стали визначальними чинниками прискорення цифрової трансформації економіки й суспільства. Значно прискорилося цифровізація великих масивів даних у різних галузях. Це передбачає їхнє переведення в машиночитний формат для оптимізації процесів збирання, зберігання та інтелектуального аналізу. Водночас ці процеси супроводжуються зростанням ризиків для безпеки та захисту персональних даних, отриманих під час онлайн-ідентифікації, автентифікації користувачів та цифровізації паперових документів. Глибока інтеграція кіберпростору в повсякденне життя перетворює цифрові профілі та онлайн-активність індивіда на невіддільну частину його особистої ідентичності [5, с. 12]. У практиці окремих держав і міжнародних організацій це сприяло формуванню концепції цифрових прав людини, метою якої є захист особи від загроз, що виникають унаслідок всеохопної цифровізації суспільства. Європа стала однією з перших у цій сфері, оскільки саме тут було закладено основи міжнародно-правового визнання та нормативного закріплення цифрових прав [6, с. 260]. Сучасне розуміння цифрового суверенітету визначається насамперед специфікою національного розвитку, географічними особливостями, а також історично сформованими практиками й інституційними традиціями, притаманними окремим регіонам [7, с. 394].

Основні регуляторні інструменти цифрового суверенітету охоплюють різні напрями цифрової політики, зокрема кібербезпеку, ШІ та цифрові послуги. Вони формують взаємопов'язану систему правового регулювання, яка дає змогу комплексно реагувати на виклики цифрової трансформації.

Таблиця 1

Основні регуляторні інструменти політики цифрового суверенітету ЄС

Регуляторний інструмент	Рік ухвалення	Сфера регулювання	Основний зміст	Інституції реалізації	Вплив на цифровий суверенітет	Практичний ефект
GDPR	2016 / 2018	Персональні дані	Захист приватності та контроль користувача над даними	Національні органи захисту даних	Посилення суверенітету даних	Підвищення довіри до цифрової економіки
Digital Services Act (DSA)	2022	Онлайн-платформи	Відповідальність платформ і прозорість алгоритмів	Єврокомісія, національні регулятори	Регулювання інформаційного простору	Боротьба з незаконним контентом
Digital Markets Act (DMA)	2022	Конкуренція	Обмеження домінування Big Tech	Європейська Комісія	Економічна автономія	Справедливі умови конкуренції
AI Act	2024	ШІ	Ризикоорієнтоване регулювання ШІ	Європейська рада з ШІ	Технологічна відповідальність	Безпечне впровадження ШІ
Data Governance Act	2022	Обмін даними	Створення спільних просторів даних	Європейська Комісія	Розвиток економіки даних	Розширення інновацій
Data Act	2023	Промислові дані	Доступ і повторне використання даних	ЄС та держави-члени	Контроль над цифровими ресурсами	Підтримка бізнесу та стартапів
NIS2 Directive	2022	Кібербезпека	Захист критичних секторів	ENISA, національні CERT	Цифрова стійкість	Зменшення кіберризиків
eIDAS Regulation	2014 / оновлення	Електронна ідентифікація	Єдина система цифрової ідентичності	Європейська Комісія	Забезпечення суверенітету цифрової ідентичності	Розвиток електронних послуг
Chips Act	2023	Напів-провідники	Розвиток виробництва мікročипів	Єврокомісія, промислові альянси	Технологічна незалежність	Зменшення зовнішньої залежності
Cybersecurity Act	2019	Сертифікація безпеки	Європейська система кіберсертифікації	ENISA	Єдині стандарти безпеки	Захист цифрових продуктів
Open Data Directive	2019	Публічні дані	Відкриття державних даних	Держави-члени ЄС	Економічна цифровізація	Розвиток цифрових сервісів
European Cloud Strategy (GAIA-X)	2020	Хмарні технології	Європейська інфраструктура даних	Консорціуми ЄС	Суверенітет інфраструктури	Альтернатива глобальним провайдерам

Джерело: розроблено авторами

Загалом політика цифрового суверенітету ЄС відображає прагнення сформувати унікальну модель цифрового розвитку, що поєднує економічну ефективність, технологічну незалежність і захист демократичних принципів. Її концептуальні засади ґрунтуються на розумінні того, що майбутня конкурентоспроможність держав визначатиметься не лише обсягом ресурсів, а й здатністю ефективно управляти цифровими процесами. Інституційні механізми гарантують координацію між різними рівнями управління, а регуляторні інструменти створюють правове середовище, адаптивне до стрімких технологічних змін. Унаслідок цього формується нова парадигма суверенітету, у якій цифровий вимір визначає економічну безпеку та стратегічний розвиток ЄС.

Європейська політика цифрової трансформації розглядається як інструмент поширення нормативного впливу ЄС на сусідні регіони, зокрема країни Східного партнерства, де інтеграція до Єдиного цифрового ринку є основним чинником модернізації державного управління та економічних систем [8, с. 1]. Дослідники підкреслюють, що цифровізація сприяє зменшенню адміністративних перешкод, розширенню доступу до цифрових послуг і формуванню умов для транскордонної електронної взаємодії, що посилює економічну та соціальну конвергенцію з ЄС [8, с. 3]. Водночас процес наближення держав Східного партнерства до стандартів ЄС супроводжується необхідністю адаптації національного законодавства у сфері захисту даних, кібербезпеки та електронної ідентифікації [8, с. 9].

У сучасних геополітичних умовах цифровий суверенітет розглядається як частина стратегічної автономії ЄС, що формується під впливом глобальної технологічної конкуренції між провідними центрами сили. Аналітичні дослідження наголошують, що ЄС прагне створити відкриту, безпечну та стійку цифрову екосистему, здатну зменшити залежність від зовнішніх технологічних платформ і забезпечити контроль над критичною цифровою інфраструктурою. Крім того, цифрова політика Союзу поєднує економічні інтереси з безпековими пріоритетами, формуючи нову модель цифрової солідарності між державами-партнерами [9].

Розвиток цифрових платформ і екосистем зумовив потребу в комплексному правовому регулюванні, спрямованому на мінімізацію ризиків для інформаційної безпеки та забезпечення справедливої конкуренції на цифрових ринках [10]. Науковці зазначають, що цифрові платформи трансформують традиційні економічні відносини, створюючи нові форми взаємодії між виробниками та споживачами, що потребує оновлення регуляторних підходів держави [10]. З огляду на це, ЄС розробляє багаторівневу систему правових механізмів, які охоплюють обіг даних, відповідальність платформ і захист цифрових прав користувачів [10].

Переосмислення категорії державного суверенітету в умовах цифровізації пов'язане з переходом від класичного територіального розуміння влади до контролю над інформаційними потоками та цифровими ресурсами [11, с. 3]. Дослідники наголошують, що інтеграційні процеси в Європі сприяють формуванню спільного цифрового простору, у межах якого суверенітет держав трансформується у форму спільного регуляторного управління [11, с. 6]. У цьому контексті цифровий суверенітет є не ізоляційною моделлю, а механізмом координації політик між державами та наднаціональними інституціями [11, с. 10].

Процес цифрової трансформації в сучасному світі визначається вже не лише технологічними інноваціями, а й нормативними межами, які формують умови функціонування цифрових ринків, захисту даних і розвитку електронного врядування. У цьому контексті ЄС є одним з основних глобальних центрів формування цифрових стандартів, що поширюються за межі його території через механізми нормативної інтеграції, економічної взаємозалежності та політичного партнерства. Країни Східного партнерства – Україна, Грузія, Молдова, Вірменія, Азербайджан і частково Білорусь – перебувають у процесі поступового наближення до європейського цифрового простору, що передбачає адаптацію правових, інституційних і технологічних підходів відповідно до *acquis* ЄС [12, с. 4].

Загалом адаптація цифрових норм ЄС у країнах Східного партнерства формує багаторівневий процес, у межах якого відбувається одночасна трансформація інституцій, економічних моделей і соціальних практик. Європейські стандарти є каталізатором реформ, однак їхня ефективність залежить від спроможності держав інтегрувати ці норми у власні політичні та економічні реалії. З огляду на це національні моделі впровадження не ідентичні, а відображають специфіку розвитку кожної країни.

Таблиця 2

**Особливості національних моделей адаптації цифрових стандартів ЄС
у країнах Східного партнерства**

Країна	Основний напрям адаптації	Інституційні особливості	Рівень інтеграції до цифрових стандартів ЄС	Основні виклики	Модель упровадження
Україна	Е-урядування, цифрова ідентифікація, кібербезпека	Активна державна цифрова політика	Високий	Безпекові ризики, війна	Прискорена інтеграційна
Грузія	Адміністративна цифровізація	Реформовані державні інституції	Високий	Обмежені ресурси	Ліберально-реформаторська
Молдова	Гармонізація законодавства	Поступова модернізація	Середній	Фінансові обмеження	Еволюційна
Вірменія	Цифрові послуги та інновації	Змішана зовнішня орієнтація	Середній	Геополітичний баланс	Гібридна
Азербайджан	Державні електронні сервіси	Централізоване управління	Помірний	Обмежена нормативна конвергенція	Державоцентрична

Джерело: розроблено авторами

Таким чином, специфіка адаптації європейських цифрових норм у країнах Східного партнерства полягає в поєднанні спільного регуляторного вектора з різними національними моделями реалізації, що формують багатовимірну архітектуру цифрової інтеграції регіону.

Реалізація політики цифрового суверенітету ЄС у контексті співпраці з державами Східного партнерства набуває особливого значення в умовах зростання цифрової взаємозалежності та посилення геополітичної конкуренції у сфері технологій. Оскільки цифровий простір поступово стає основою економічної стабільності, державної безпеки та соціальної стійкості, виникає потреба у створенні ефективних механізмів інтеграції країн-партнерів до європейської цифрової екосистеми. Водночас наближення до стандартів ЄС супроводжується комплексом викликів, які пов'язані як із внутрішніми трансформаціями держав, так і із зовнішніми ризиками, що впливають на їхню цифрову політику [13, с. 110].

Одним з основних викликів є нерівномірність цифрового розвитку країн Східного партнерства. Відмінності в технологічній інфраструктурі, доступі до інвестицій та цифрових навичках населення створюють асиметрію можливостей щодо впровадження європейських стандартів. За наявності значного прогресу в розвитку електронного врядування та цифрових сервісів в окремих державах інші постають перед проблемами модернізації базової інфраструктури та інституційної координації. Це ускладнює формування єдиного регуляторного простору та потребує диференційованого підходу ЄС [14, с. 55].

Перспективи реалізації політики цифрового суверенітету пов'язані насамперед із формуванням спільного цифрового простору, у межах якого країни-партнери отримують доступ до технологічних ресурсів, програм розвитку та інституційної підтримки ЄС. Поглиблення інтеграції сприяє підвищенню якості державного управління, розвитку електронної демократії та створенню нових економічних можливостей. У довгостроковій перспективі цифровий суверенітет може стати інструментом зміцнення регіональної стабільності, оскільки забезпечує не лише технологічну незалежність, а й формування спільних правил цифрової взаємодії [15, с. 77].

Таблиця 3

**Виклики, ризики та перспективи реалізації політики цифрового суверенітету
в країнах Східного партнерства**

Напрямок оцінки	Основні прояви	Структурні причини	Потенційні ризики	Інструменти реагування ЄС	Очікувані перспективи	Довгостроковий ефект
Інфраструктурний розвиток	Розбудова широко-смугового доступу, цифрових платформ, дата-центрів	Нерівномірний рівень технологічного розвитку	Цифровий розрив між країнами та регіонами	Програми Digital Europe, інвестиційні фонди ЄС	Розширення доступу до цифрових послуг	Формування інтегрованого цифрового ринку

Продовження таблиці 3

Кібербезпека	Упровадження стандартів кіберзахисту	Зростання гібридних загроз	Кібератаки на критичну інфраструктуру	Співпраця з ENISA, імплементація NIS-стандартів	Підвищення цифрової стійкості	Зміцнення національної безпеки
Інституційна адаптація	Гармонізація законодавства з <i>acquis</i> ЄС	Недостатня адміністративна спроможність	Формальне виконання норм без практичної ефективності	Технічна допомога, Twinning-проекти	Підвищення якості державного управління	Конвергенція управлінських моделей
Економічна інтеграція	Участь у цифровій торгівлі та сервісах	Обмежені ресурси малого бізнесу	Посилення конкуренції з європейськими компаніями	Програми підтримки МСП, інноваційні гранти	Залучення інвестицій	Інтеграція в ланцюги доданої вартості ЄС
Регулювання даних	Упровадження стандартів захисту персональних даних	Недосконалість правових механізмів	Витік даних, зниження довіри користувачів	Адаптація GDPR, створення наглядових органів	Безпечний обіг інформації	Формування економіки даних
Соціально-цифровий розвиток	Розвиток е-послуг та цифрових навичок	Нерівний доступ до освіти та технологій	Соціальна нерівність і цифрове вилучення	Освітні програми та цифрові ініціативи ЄС	Підвищення цифрової грамотності	Інклюзивна цифрова трансформація
Політична стабільність	Цифровізація публічного управління	Вплив зовнішніх інформаційних кампаній	Маніпуляції інформацією	Регулювання платформ, боротьба з дезінформацією	Підвищення прозорості влади	Посилення демократичних інститутів
Технологічна залежність	Використання іноземних ІТ-рішень	Відсутність власних технологічних екосистем	Залежність від зовнішніх постачальників	Розвиток європейських технологічних партнерств	Диверсифікація технологій	Часткове досягнення цифрової автономії
Інноваційний розвиток	Підтримка стартапів і цифрових кластерів	Недостатній доступ до капіталу	Відтік талантів	Horizon Europe, інноваційні хаби	Зростання ІТ-сектору	Формування регіональних інноваційних центрів

Джерело: розроблено авторами

Упровадження європейських цифрових стандартів сприяє формуванню спільного нормативного простору, який підвищує довіру до цифрових сервісів, стимулює інноваційний розвиток і створює передумови для економічної конвергенції з ЄС. Водночас цифрова трансформація посилює вимоги до кібербезпеки, управління даними та розвитку людського капіталу, що робить політику цифрового суверенітету визначальним чинником довгострокової стійкості. У стратегічній перспективі саме поєднання регуляторної інтеграції, технологічного розвитку й інституційного зміцнення здатне забезпечити послідовне долучення держав Східного партнерства до європейської цифрової екосистеми та формування спільного простору цифрової довіри.

Висновки. У дослідженні встановлено, що політика цифрового суверенітету ЄС є комплексною моделлю стратегічної автономії, яка поєднує економічні, правові та безпекові інструменти регулювання цифрового середовища. Її інституційна архітектура заснована на системі взаємопов'язаних регуляторних актів, спрямованих на захист даних, гарантування кібербезпеки, розвиток економіки даних і обмеження технологічної залежності, що свідчить про трансформацію традиційного розуміння суверенітету в цифровому вимірі.

Доведено, що імплементація європейських цифрових норм у країнах Східного партнерства має асиметричний характер і визначається національними інституційними можливостями, рівнем цифрового розвитку та безпековими умовами. Виявлено варіативність моделей адаптації – від прискореної інтеграційної до еволюційної та державоцентричної, що підтверджує відсутність універсального сценарію цифрової конвергенції з ЄС.

З'ясовано, що реалізація політики цифрового суверенітету створює значні можливості для модернізації державного управління, розвитку електронних послуг і підвищення цифрової стійкості, але супроводжується ризиками технологічної залежності, кіберзагроз, інституційних обмежень і цифрового розриву. Обґрунтовано, що цифровий суверенітет є основним інструментом інтеграції держав Східного партнерства до європейського цифрового простору та формування спільної екосистеми цифрової довіри.

Перспективи подальших досліджень пов'язані з поглибленим порівняльним аналізом

ефективності імплементації окремих регуляторних актів ЄС у країнах Східного партнерства, кількісною оцінкою впливу цифрової інтеграції на економічну та безпекову стійкість держав, а також із вивченням взаємозв'язку між розвитком цифрових прав, інноваційних екосистем і формуванням технологічної автономії регіону. Особливої уваги потребує вивчення ролі ШІ, хмарних інфраструктур і транскордонного управління даними як чинників майбутньої цифрової конвергенції з ЄС.

Література

1. Голуб'як І., Голуб'як Н. Політичні ініціативи ЄС для підтримки розвитку інформаційного суспільства. *Вісник Прикарпатського університету. Серія: Політологія : спецвипуск з нагоди 60-літнього ювілею професора Ігоря Цепенди*. 2024. № 18. С. 92–100. DOI: <https://doi.org/10.32782/2312-1815/2024-18-10>
2. Петришина М. О., Балабан М. М. Підходи ЄС до формування цифрового суверенітету: досвід Естонії для України. *Український політико-правовий дискурс*. 2025. № 10. DOI: <https://doi.org/10.5281/zenodo.15306095>
3. Калюжна Ю. І. Цифровий суверенітет як фактор національної безпеки ЄС та України. *Національні інтереси України*. 2025. № 6(11). С. 1094–1124. DOI: [https://doi.org/10.52058/3041-1793-2025-6\(11\)-1094-1124](https://doi.org/10.52058/3041-1793-2025-6(11)-1094-1124)
4. Floridi L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*. 2020. №. 33. P. 369–378. URL: <https://link.springer.com/article/10.1007/s13347-020-00423-6> (дата звернення: 01.02.2026).
5. Tan K. L., Chi C. H., Lam K. Y. Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys*. 2023. Vol. 56, № 3. P. 1–36. URL: <https://dl.acm.org/doi/abs/10.1145/3616400>.
6. Лабик А. Р., Строїч М. І., Ліка М. І. Виклики міжнародно-правової регламентації права на забуття в Інтернеті. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. Вип. 86. Ч. 5. С. 258–263. DOI: <https://doi.org/10.24144/2307-3322.2024.86.5.39>
7. Лабик А. Р., Яремчук В. В. Концепція цифрового суверенітету держави: міжнародно-правовий аспект. *Юридичний науковий електронний журнал*. 2025. № 2. С. 393–395. DOI: <https://doi.org/10.32782/2524-0374/2025-2/92>
8. Tsebenko O., Ivasechko O., Turchyn Y., Holoshchuk R. EU Digital Market: the Future of Eastern Partnership. *CEUR Workshop Proceedings*. 2023. Vol. 3296. P. 1–14. URL: <https://ceur-ws.org/Vol-3296/paper1.pdf> (date of access: 01.02.2026).
9. Гнатюк С. Геополітичне цифрове візіонерство США та ЄС: цифрова солідарність, цифровий суверенітет і нова американська стратегія розвитку міжнародного кіберпростору. *НІСД: вебсайт*. 2025. URL: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/heopolitychne-tyfrove-vizionerstvo-ssha-ta-yes-tyfrova> (дата звернення: 01.02.2026).
10. Корват О. В. Формування державної політики у сфері цифрових платформ і екосистем. *Право та інновації*. 2023. № 3 (43). С. 83–88. DOI: [https://doi.org/10.37772/2518-1718-2023-3\(43\)-11](https://doi.org/10.37772/2518-1718-2023-3(43)-11)
11. Солодка О. М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. № 1(32). С. 80–87. DOI: [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311)
12. Zaiats N., Rega I., Boiko V., Shlieina L., Toporkova M. Ensuring gender equality and legal protection of women's rights: achievements, challenges, and prospects. *Multidisciplinary Science Journal*. 2024. Vol. 6. Article 2024ss0202. DOI: <https://doi.org/10.31893/multiscience.2024ss0202>
13. Лисянський П. Л., Саліхов А. Р., Ястребова В. А. Зовнішній вплив РФ на виборчі кампанії у інших країнах. *Регіональні студії : науковий збірник*. 2024. Вип. 39. С. 106–113. URL: <http://regionalstudies.uzhnu.uz.ua/archive/39/19.pdf> (дата звернення: 01.02.2026).
14. Лисянський П. Діяльність профспілкових організацій РФ на тимчасово окупованих територіях України як інструмент посилення політики експансіонізму. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № 3(75). С. 51–57. DOI: [https://doi.org/10.32689/2523-4625-2024-3\(75\)-8](https://doi.org/10.32689/2523-4625-2024-3(75)-8)
15. Khotynska N. Prospects and challenges in implementing comprehensive assistance programs for vulnerable populations in the USA. *European Journal of Interdisciplinary Issues*. 2024. Vol. 1, № 1. P. 75–81. DOI: <https://doi.org/10.5281/zenodo.14791395>

References

1. Holubiak I., Holubiak N. (2024) Politychni initsiatyvy YeS dlia pidtrymky rozvytku informatsiinoho suspilstva [EU political initiatives to support the development of the information society]. *Visnyk Prykarpatskoho universytetu. Serii: Politolohiia*, no. 18, pp. 92–100. DOI: <https://doi.org/10.32782/2312-1815/2024-18-10> (accessed February 22, 2026).

2. Petryshyna M. O., Balaban M. M. (2025) PidkhodyeS do formuvannia tsyfrovoho suverenitetu: dosvid Estonii dlia Ukrainy [EU approaches to digital sovereignty formation: Estonia's experience for Ukraine]. *Ukrainskyi polityko-pravovyi dyskurs*, no. 10. DOI: <https://doi.org/10.5281/zenodo.15306095> (accessed February 22, 2026).
3. Kaliuzhna Yu. I. (2025) Tsyfrovyyi suverenitet yak faktor natsionalnoi bezpeky YeS ta Ukrainy [Digital sovereignty as a factor of national security of the EU and Ukraine]. *Natsionalni interesy Ukrainy*, vol. 6, no. 11, pp. 1094–1124. DOI: [https://doi.org/10.52058/3041-1793-2025-6\(11\)-1094-1124](https://doi.org/10.52058/3041-1793-2025-6(11)-1094-1124) (accessed February 23, 2026).
4. Floridi L. (2020) The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, no. 33, pp. 369–378. Available at: <https://link.springer.com/article/10.1007/s13347-020-00423-6> (accessed February 01, 2026).
5. Tan K. L., Chi C. H., Lam K. Y. (2023) Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–36. Available at: <https://dl.acm.org/doi/abs/10.1145/3616400> (accessed February 01, 2026).
6. Labyk A. R., Stroich M. I., Ilika M. I. (2024) Vyklyky mizhnarodno-pravovoi rehlamentatsii prava na zabuttia v Interneti [Challenges of international legal regulation of the right to be forgotten on the Internet]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriya Pravo*, vol. 86, no. 5, pp. 258–263. DOI: <https://doi.org/10.24144/2307-3322.2024.86.5.39> (accessed February 01, 2026).
7. Labyk A. R., Yaremchuk V. V. (2025) Kontseptsiia tsyfrovoho suverenitetu derzhavy: mizhnarodno-pravovyi aspekt [The concept of digital sovereignty of the state: international legal aspect]. *Yurydychnyi naukovyi elektronnyi zhurnal*, no. 2. pp. 393–395. DOI: <https://doi.org/10.32782/2524-0374/2025-2/92> (accessed February 01, 2026).
8. Tsebenko O., Ivasechko O., Turchyn Y., Holoshchuk R. (2023) EU Digital Market: the Future of Eastern Partnership. *CEUR Workshop Proceedings*, vol. 3296, pp. 1–14. Available at: <https://ceur-ws.org/Vol-3296/paper1.pdf> (accessed February 01, 2026).
9. Hnatiuk S. (2025) Hnatiuk S. Heopolitychne tsyfrove vizionerstvo SShA ta YeS: tsyfrova solidarist, tsyfrovyyi suverenitet i nova amerykanska stratehiia rozvytku mizhnarodnoho kiberprostoru [Geopolitical digital visionary of the USA and the EU: digital solidarity, digital sovereignty and the new American strategy for the development of international cyberspace]. *NISD: vebseit*. Available at: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/heopolitychne-tyfrove-vizionerstvo-ssha-ta-yes-tyfrova> (accessed February 01, 2026).
10. Korvat O. V. (2024) Formuvannia derzhavnoi polityky u sferi tsyfrovyykh platform i ecosystem [Formation of state policy in the field of digital platforms and ecosystems]. *Pravo ta innovatsii*, vol. 3, no. 43, pp. 83–88. DOI: [https://doi.org/10.37772/2518-1718-2023-3\(43\)-11](https://doi.org/10.37772/2518-1718-2023-3(43)-11) (accessed February 01, 2026).
11. Solodka O. M. (2020) Zabezpechennia informatsiinoho suverenitetu derzhavy: pravovyyi dyskurs [Ensuring information sovereignty of the state: legal discourse]. *Informatsiia i pravo*, vol. 1, no. 32, pp. 80–87. DOI: [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311) (accessed February 01, 2026).
12. Zaiats N., Rega I., Boiko V., Shlieina L., Toporkova M. (2024) Ensuring gender equality and legal protection of women's rights: achievements, challenges, and prospects. *Multidisciplinary Science Journal*, vol. 6, article 2024ss0202. DOI: <https://doi.org/10.31893/multiscience.2024ss0202> (accessed February 01, 2026).
13. Lysianskyi P. L., Salikhov A. R., Yastrebova V. A. (2024) Zovnishnii vplyv RF na vyborchi kampanii u inshykh krainakh [External influence of the Russian Federation on electoral campaigns in other countries]. *Rehionalni studii*, no. 39, pp. 106–113. Available at: <http://regionalstudies.uzhnu.uz.ua/archive/39/19.pdf> (accessed February 01, 2026).
14. Lysianskyi P. (2024) Diialnist profspilkovykh orhanizatsii RF na tymchasovo okupovanykh terytoriiakh Ukrainy yak instrument posylennia polityky ekspansionizmu [Activities of trade union organizations of the Russian Federation in temporarily occupied territories of Ukraine as an instrument of expansionist policy]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia*, vol. 3, no. 75, pp. 51–57. DOI: [https://doi.org/10.32689/2523-4625-2024-3\(75\)-8](https://doi.org/10.32689/2523-4625-2024-3(75)-8) (accessed February 01, 2026).
15. Khotynska N. (2024) Prospects and challenges in implementing comprehensive assistance programs for vulnerable populations in the USA. *European Journal of Interdisciplinary Issues*, vol. 1, no. 1, pp. 75–81. DOI: <https://doi.org/10.5281/zenodo.14791395> (accessed February 01, 2026).

Отримано: 02.02.2026

Прийнято до публікації: 02.03.2026

Опубліковано: 15.03.2026