

УДК 35.072.6:004.738.5

Михайлов Сергій Юрійович

аспірант кафедри державного управління

Навчально-наукового інституту публічного управління та державної служби

Київського національного університету імені Тараса Шевченка

Mykhailov Serhii

Postgraduate Student of the Department of Public Administration

Educational and Scientific Institute of Public Administration and Civil Service of

Taras Shevchenko National University of Kyiv

ORCID: 0009-0000-1437-2292

DOI: 10.25313/2617-572X-2025-5-10957

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ В ПУБЛІЧНОМУ УПРАВЛІННІ УКРАЇНИ: ЄВРОПЕЙСЬКІ ОРІЄНТИРИ

INSTITUTIONAL SUPPORT FOR DIGITAL SOVEREIGNTY IN PUBLIC ADMINISTRATION OF UKRAINE: EUROPEAN GUIDELINES

Анотація. Вступ. У контексті глобальної цифровізації, зростаючої залежності держав від транснаціональних технологічних корпорацій, а також активізації кіберзагроз і гібридних впливів, проблема забезпечення цифрового суверенітету набуває особливого значення для країн, що перебувають у процесі демократичного та технологічного становлення. Для України, яка веде боротьбу за політичну незалежність і водночас здійснює інтенсивну цифрову трансформацію, формування дієвої системи цифрового суверенітету є критично важливим завданням державного управління. Пошук оптимальної моделі інституційного забезпечення цифрового суверенітету, з урахуванням успішного досвіду Європейського Союзу, постає як ключовий напрям публічної політики.

Мета. Стаття має на меті проаналізувати сутність поняття цифрового суверенітету та його значення в контексті публічного управління, визначити інституційні засади забезпечення цифрового суверенітету в ЄС, оцінити стан інституційного забезпечення цифрового суверенітету в Україні та розробити пропозиції щодо адаптації європейських практик для українських реалій.

Матеріали і методи. Методологічну основу дослідження становлять структурно-функціональний, інституційний, порівняльно-правовий аналіз, контент-аналіз нормативних актів та стратегічних документів, а також елементи емпіричного аналізу, зокрема вивчення міжнародних рейтингів та звітів галузевих інституцій. Джерельну базу склали акти законодавства України та ЄС, аналітичні звіти, державні програми, дані міжнародних індексів (GCI, EGDI, DESI тощо).

Результати. У статті уточнено зміст категорії «цифровий суверенітет» як складової національного суверенітету в умовах цифрової трансформації. Проаналізовано ключові інституційні компоненти європейської моделі цифрового суверенітету, такі як GAIA-X, Chips Act, політика кібербезпеки ЄС, Horizon Europe. Проведено оцінку стану інституційного забезпечення цифрового суверенітету в Україні, виявлено як позитивні зрушення, зокрема розвиток цифрових сервісів, нормативне закріплення кібербезпеки, так і проблемні аспекти – залежність від іноземних хмарних платформ, фрагментарність законодавства, обмежена координація цифрової політики. Запропоновано напрями адаптації європейських підходів з урахуванням українських викликів, серед яких: розширення інституційної спроможності державних органів, імплементація принципів суверенного зберігання даних, розвиток власної технологічної інфраструктури.

Перспективи. Подальші дослідження доцільно зосередити на вивченні механізмів публічно-приватного партнерства у формуванні цифрового суверенітету, а також на оцінці ефективності інтеграції України у європейський цифровий простір у контексті майбутнього членства в ЄС. Також актуальним є моніторинг впровадження законодавства у сфері кібербезпеки та цифрових прав громадян.

Ключові слова: кіберзагроза, гібридний вплив, інформаційний простір, технологічні виклики.

Summary. Introduction. In the context of global digitalization, the growing dependence of states on transnational technology corporations, as well as the intensification of cyber threats and hybrid influences, the problem of ensuring digital sovereignty is of particular importance for countries in the process of democratic and technological formation. For Ukraine, which is fighting for political independence and at the same time carrying out intensive digital transformation, the formation of an effective system of digital sovereignty is a critically important task of public administration. The search for the optimal model of institutional support for digital sovereignty, taking into account the successful experience of the European Union, appears as a key direction of public policy.

Purpose. The article aims to analyze the essence of the concept of digital sovereignty and its significance in the context of public administration, to determine the institutional principles of ensuring digital sovereignty in the EU, to assess the state of institutional support for digital sovereignty in Ukraine and to develop proposals for adapting European practices to Ukrainian realities.

Materials and methods. The methodological basis of the study is structural-functional, institutional, comparative-legal analysis, content analysis of regulatory acts and strategic documents, as well as elements of empirical analysis, in particular, the study of international ratings and reports of industry institutions. The source base was made up of acts of Ukrainian and EU legislation, analytical reports, state programs, data from international indices (GCI, EGDI, DESI, etc.).

Results. The article clarifies the content of the category "digital sovereignty" as a component of national sovereignty in the context of digital transformation. The key institutional components of the European model of digital sovereignty are analyzed, such as GAIA-X, Chips Act, EU cybersecurity policy, Horizon Europe. An assessment of the state of institutional support for digital sovereignty in Ukraine was conducted, revealing both positive developments, in particular the development of digital services, regulatory consolidation of cybersecurity, and problematic aspects – dependence on foreign cloud platforms, fragmentation of legislation, limited coordination of digital policy. Directions for adapting European approaches taking into account Ukrainian challenges are proposed, including: expanding the institutional capacity of state bodies, implementing the principles of sovereign data storage, developing our own technological infrastructure.

Prospects. Further research should be focused on studying the mechanisms of public-private partnership in the formation of digital sovereignty, as well as on assessing the effectiveness of Ukraine's integration into the European digital space in the context of future membership in the EU. Monitoring the implementation of legislation in the field of cybersecurity and digital rights of citizens is also relevant.

Key words: cyber threat, hybrid influence, information space, technological challenges.

Постановка проблеми. У сучасних умовах цифрової трансформації суспільства та державного управління питання цифрового суверенітету набуває особливої актуальності. В умовах зростання кіберзагроз, гібридних впливів та залежності від іноземних цифрових платформ постає необхідність створення ефективної інституційної системи, здатної забезпечити захист інформаційного простору, збереження контролю над цифровими ресурсами та гарантування національного інтересу в цифровій сфері. Україна, яка декларує курс на європейську інтеграцію, зобов'язана враховувати європейські підходи до забезпечення цифрового суверенітету, які поєднують інноваційний розвиток, прозорість, дотримання прав людини та стратегічну автономію. Проте на сьогодні відсутня цілісна модель інституційного забезпечення цифрового суверенітету в публічному управлінні, що ускладнює реалізацію ефективної цифрової політики, знижує стійкість держави до зовнішніх технологічних викликів і гальмує гармонізацію з європейськими стандартами. Це зумовлює потребу у науковому аналізі існуючих викликів, оцінці стану інституційного середовища та формуванні рекомендацій щодо його удосконалення з урахуванням європейського досвіду.

Аналіз останніх досліджень і публікацій. У вітчизняному та зарубіжному науковому дискурсі цифровий суверенітет дедалі частіше розглядається як базовий компонент державної безпеки, самостійності в кіберпросторі та ефективності публічного управління. Водночас аналіз наявної наукової літератури

засвідчує, що питання інституційного забезпечення цифрового суверенітету залишається фрагментарно висвітленим, особливо в українському контексті.

Серед сучасних дослідників важливим є внесок Ю. П. Калайди [1], який здійснив порівняльний аналіз моделей цифрового суверенітету, сформованих у провідних демократичних країнах. Автор підкреслює, що в умовах геополітичного протистояння цифровий суверенітет виходить за межі технічного або правового явища, набуваючи стратегічного значення. У роботі систематизовано закордонний досвід (насамперед ЄС, США, Китаю) щодо захисту даних, розвитку національної хмарної інфраструктури та посилення кібербезпеки, проте потребує подальшої конкретизації питання імплементації подібних моделей в українських умовах.

І. М. Доронін [2] зосереджується на юридичних колізіях, що виникають у процесі «суверенізації Інтернету». Дослідник звертає увагу на конфлікт між прагненням держави до контролю над цифровим простором і необхідністю збереження відкритості глобальної мережі, що обумовлює складність формування єдиної моделі цифрового суверенітету. Його висновки актуалізують проблему балансування між технологічною автономією та дотриманням міжнародних стандартів прав людини.

О. М. Солодка [3] розкриває проблематику інформаційного суверенітету через правовий дискурс, зокрема акцентуючи на законодавчому регулюванні сфер інформаційної безпеки, збереження

персональних даних та інформаційної незалежності. Її підхід дозволяє розглядати цифровий суверенітет як логічне продовження інформаційного, однак не дає повного уявлення про інституційну структуру забезпечення останнього.

Зовнішньополітичний вимір цифрового суверенітету ґрунтовно аналізує С. Гнатюк [4]. У фокусі його дослідження — цифрове візіонерство ЄС і США, їхні підходи до регуляції інтернет-простору, побудови цифрової інфраструктури та стратегій кіберзахисту. Автор окреслює концепцію «цифрової солідарності» як інструмент інтеграції цифрових політик демократичних країн, що становить інтерес у контексті прагнення України до євроінтеграції.

І. М. Милосердна [5] аналізує сучасні інтерпретації поняття цифрового суверенітету та ступінь їх відображення у практичних кроках державної політики. Авторка наголошує на розриві між науковою риторикою та реальним станом речей у сфері цифрової незалежності України, вказуючи на нестачу системного підходу та узгодженої нормативно-правової бази.

У більш ранній роботі Д. В. Дубова [6] цифровий суверенітет розглядається як новий тип національного суверенітету, що формується під впливом цифрових технологій і глобальних інформаційних потоків. Він визначає низку викликів для України, серед яких — технічна залежність, слабка інституційна спроможність та потреба в адаптації найкращих практик. Водночас його дослідження є радше концептуальним, без глибокого аналізу конкретних управлінських інструментів.

К. В. Єфремова [7] підкреслює роль цифрового суверенітету як ключового чинника конкурентоспроможності держави в умовах Індустрії 4.0. Вона наголошує на необхідності побудови власної цифрової екосистеми, здатної забезпечити автономне функціонування критичної інфраструктури. Її напрацювання є цінними для формування інституційної платформи цифрового суверенітету, однак потребують розширення в напрямі публічно-управлінських аспектів.

У зарубіжному науковому полі вартим уваги є дослідження А. Баррінья, Г. Крістоу (A. Barrinha, G. Christou) [8], які аналізують європейську політику цифрового суверенітету як форму стратегічного самоствердження в кіберпросторі. Автори вказують на формування окремої «мови суверенітету», що дозволяє ЄС артикулювати свої інтереси в діджитал-сфері через створення нормативної бази, інституційних структур і технічних стандартів. Їхні висновки підкреслюють складність поєднання політичної волі та технічної реалізації цифрової автономії.

Отже, незважаючи на наявність низки цінних досліджень, залишається недостатньо розкритим комплекс питань, пов'язаних із практичною інституціоналізацією цифрового суверенітету в системі публічного управління України. Зокрема, вкрай обмежено представлені дослідження щодо порівняння

інституційної моделі ЄС з українською дійсністю, а також відсутні узагальнення щодо адаптації європейських управлінських практик до українських умов. Саме заповнення цих прогалин і визначено як мету цього дослідження.

Метою статті є дослідження інституційних засад формування та реалізації цифрового суверенітету в системі публічного управління України з урахуванням європейських підходів, а також розроблення науково обґрунтованих рекомендацій щодо імплементації ефективної моделі цифрового суверенітету в національну управлінську практику.

Завдання статті:

- проаналізувати сутність поняття цифрового суверенітету та його значення в контексті публічного управління;
- визначити основні інституційні складові цифрового суверенітету в європейському управлінському просторі;
- оцінити стан інституційного забезпечення цифрового суверенітету в Україні;
- розробити пропозиції щодо адаптації та впровадження європейських практик забезпечення цифрового суверенітету в Україні.

Матеріали і методи. У процесі дослідження використано комплекс загальнонаукових і спеціальних методів, що дозволили здійснити ґрунтовний аналіз цифрового суверенітету як складної категорії публічного управління. Основу джерельної бази становили чинні нормативно-правові акти України та Європейського Союзу, зокрема Регламент (ЄС) 2016/679 (GDPR), Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України (2021–2025), законопроекти, програмні документи ЄС (наприклад, Digital Decade 2030, GAIA-X, Chips Act, Data Governance Act) та відповідні урядові постанови.

Метод структурно-функціонального аналізу застосовано для виявлення інституційних елементів цифрового суверенітету та аналізу їх взаємозв'язків у європейській та українській практиках. Порівняльно-правовий метод дозволив зіставити підходи до інституційного забезпечення цифрового суверенітету в ЄС та Україні, визначити загальні риси та відмінності. У ході дослідження також застосовано системний підхід для комплексного розуміння сутності цифрового суверенітету та можливостей його інституційного забезпечення в умовах трансформацій сучасного глобального цифрового простору.

Виклад основного матеріалу. У сучасних умовах стрімкої цифровізації усіх сфер суспільного життя проблема цифрового суверенітету набуває особливої актуальності як з точки зору національної безпеки, так і в контексті ефективного функціонування системи публічного управління. Традиційно поняття суверенітету трактується як верховенство держави, народу або нації у внутрішній та зовнішній політиці, що забезпечує самостійність прийняття

рішень та реалізацію стратегічних цілей [9]. У науковій літературі виділяють три основні типи суверенітету — державний, народний і національний, кожен з яких має свого суб'єкта: відповідно, державу, народ та націю. У межах мононаціональних держав ці види суверенітету можуть збігатися, що спрощує питання управління, тоді як у багатонаціональних державах відбувається постійна взаємодія, узгодження та, подекуди, конфлікт між ними. У цьому контексті державний суверенітет відіграє ключову роль як юридично та політично оформлений механізм реалізації народного волевиявлення, що охоплює як внутрішню автономію державної влади, так і її незалежність у зовнішньополітичних стосунках.

З утвердженням інформаційного суспільства традиційне розуміння державного суверенітету, що спирається на територіальні межі юрисдикції, зазнає суттєвих трансформацій. Глобальні інформаційні потоки, кіберзалежність, розвиток транснаціональних цифрових платформ та систем штучного інтелекту розмивають межі між внутрішнім і зовнішнім простором функціонування держави. У зв'язку з цим у науковий обіг активно входять поняття «інформа-

ційний суверенітет» і «цифровий суверенітет». Інформаційний суверенітет розглядається як здатність держави контролювати, регулювати та захищати національні інформаційні ресурси та інформаційні потоки на своїй території [10]. Він передбачає наявність інституційних механізмів з протидії інформаційно-психологічним впливам, забезпечення автономії національної інформаційної політики та створення умов для безпечного функціонування вітчизняного інформаційного простору.

Цифровий суверенітет є логічним розвитком концепції інформаційного суверенітету, зосередженим переважно на аспектах незалежності у сфері інформаційно-комунікаційних технологій (ІКТ), інфраструктури цифрового управління, кібербезпеки, збереження та обробки персональних даних, а також на цифровій інфраструктурі, через яку здійснюється реалізація управлінських функцій. Він полягає у здатності держави самостійно визначати цифрову політику, керувати розвитком та захистом цифрових систем, гарантувати недопущення зовнішнього втручання у критичні елементи цифрового середовища, включно з державними реєстрами, каналами

Таблиця 1

Функції цифрового суверенітету у публічному секторі

Зміст функції	Значення для публічного управління
<i>Нормативно-регуляторна</i>	
Формування та впровадження законодавчої та регуляторної бази, що визначає правила цифрової діяльності.	Забезпечує контроль над цифровими процесами, легітимізує втручання держави у сферу ІКТ і платформ.
<i>Юрисдикційна</i>	
Встановлення меж державної юрисдикції у цифровому просторі.	Гарантує право держави визначати, хто і як може здійснювати цифрову діяльність у її інформаційно-комунікаційному полі.
<i>Кібербезпекова</i>	
Створення умов для захисту інформаційної інфраструктури від зовнішніх і внутрішніх загроз.	Сприяє безпеці критичних об'єктів, запобігає втраті контролю над цифровими платформами, даними, системами управління.
<i>Технологічно-інфраструктурна</i>	
Розвиток власної цифрової інфраструктури, включно з дата-центрами, хмарними сервісами, національними мережами.	Знижує залежність від іноземних технологій, підтримує цифрову автономію та стійкість у кризових ситуаціях.
<i>Координаційна</i>	
Узгодження дій державних інституцій, бізнесу та громадянського суспільства в цифровій сфері.	Створює єдину цифрову політику, забезпечує узгоджене управління цифровою трансформацією.
<i>Інформаційно-комунікаційна</i>	
Регулювання інформаційних потоків, протидія дезінформації, контроль над інформаційним простором.	Забезпечує національну інформаційну безпеку, зменшує вплив зовнішніх інформаційно-психологічних операцій.
<i>Економічна</i>	
Створення умов для розвитку національного цифрового ринку та зменшення цифрової залежності від іноземних акторів.	Підвищує інноваційність публічного сектору, зберігає цифрову ренту у межах держави.
<i>Освітньо-культурна</i>	
Сприяння формуванню цифрової культури, медіаграмотності та цифрової свідомості населення.	Забезпечує стійкість суспільства до маніпуляцій, сприяє інклюзивності та ефективному управлінню цифровими змінами.

Джерело: власна розробка автора

комунікації, платформами публічного управління та системами електронного урядування.

Значення цифрового суверенітету в контексті публічного управління полягає передусім у створенні передумов для формування незалежної, стабільної та безпечної цифрової держави, спроможної забезпечити захист громадян в інформаційному середовищі, збереження цілісності цифрових процесів управління та мінімізацію ризиків цифрової колонізації через надмірну залежність від іноземних технологій або нормативних режимів. У публічному секторі цифровий суверенітет дозволяє підвищити прозорість та підзвітність управлінських процесів, забезпечити безперебійну роботу електронних послуг, захист персональних даних громадян, унеможливити втручання в інфраструктуру державного управління та забезпечити стратегічний контроль над критичною цифровою інфраструктурою.

У цьому контексті доцільно виокремити ключові функції цифрового суверенітету у публічному секторі, які визначають його системну роль у забезпеченні ефективного, безпечного та незалежного державного управління в цифрову епоху. Таблиця 1 узагальнює основні напрями реалізації цифрового суверенітету на рівні державних інституцій.

У контексті загострення геополітичного протистояння та швидкого розвитку цифрових технологій, формування концепції цифрового суверенітету набуває ключового значення в управлінських практиках сучасного Європейського Союзу. ЄС дедалі активніше позиціонує себе як незалежний глобальний суб'єкт, здатний забезпечити контроль над власною цифровою інфраструктурою, інформаційними потоками та технологічною політикою. Це прагнення до суверенізації цифрового простору не є ізольованим випадком, а частиною ширшої європейської стратегії автономізації в умовах нової реальності — постамериканського, багатопольярного цифрового світу. Відтак, цифровий суверенітет розглядається не лише як технічна або правова категорія, а як стратегічна управлінська мета, що вимагає створення відповідної інституційної архітектури на рівні ЄС та його держав-членів.

Основними інституційними складовими цифрового суверенітету в європейському управлінському просторі виступають: Європейська комісія, відповідальні агентства з питань цифрових технологій та кібербезпеки (зокрема, Європейське агентство з кібербезпеки — ENISA), Європейська рада з питань цифрового десятиліття, а також національні органи регулювання в державах-членах. Ключову роль відіграє Європейська комісія, яка не лише ініціює відповідні законодавчі акти, але й забезпечує стратегічне планування, моніторинг реалізації цифрової політики, а також координацію міждержавних дій у сфері цифрової трансформації. Зокрема, такі ініціативи, як Digital Services Act (DSA), Digital Markets Act (DMA), Data Governance Act (DGA) та Європейська

декларація про цифрові права і принципи, мають не лише нормативну, а й інституційну функцію — вони закладають підґрунтя для формування єдиної європейської цифрової юрисдикції.

ENISA, зі свого боку, виконує функції експертного, консультативного й координаційного центру у сфері забезпечення кіберстійкості та управління ризиками цифрового середовища. Вона активно взаємодіє з національними органами кібербезпеки та бере участь у формуванні спільних стандартів та методик для країн-членів ЄС. Іншим важливим елементом є платформи багаторівневої координації, які формуються на основі Стратегії цифрового десятиліття ЄС — 2030 [ґнідий]. У рамках цієї стратегії створено механізм співпраці між інституціями ЄС і державами-членами з метою досягнення чотирьох ключових цілей: розвиток цифрових навичок, цифрової інфраструктури, цифровізації бізнесу та електронного урядування. Таким чином, формується комплексна інституційна модель, що передбачає як вертикальну (інституції ЄС — держави-члени), так і горизонтальну (між-агентську та міждержавну) інтеграцію.

Особливу увагу в європейській моделі цифрового суверенітету приділено питанням локалізації даних та розвитку стратегічно важливих технологій. Для цього ЄС просуває такі ініціативи, як GAIA-X — федеративна європейська хмарна інфраструктура, спрямована на зменшення залежності від американських і китайських технологічних гігантів. У свою чергу, Інвестиційна програма Horizon Europe та нова Ініціатива Chips Act мають на меті підтримку інновацій, R&D, розвиток власного напівпровідникового виробництва та цифрових індустрій, що також прямо пов'язано з забезпеченням суверенітету у високотехнологічному вимірі. Крім того, не менш важливим інструментом є політика кібербезпеки, що охоплює як нормативно-правові документи, так і інфраструктурні проекти, зокрема спільні платформи для виявлення, реагування та протидії кіберзагрозам.

Таким чином, формування цифрового суверенітету Європейського Союзу базується на багаторівневому та комплексному підході, що охоплює технологічний розвиток, захист персональних даних, інноваційне виробництво та кібербезпеку. Реалізація відповідних стратегій потребує ефективної координації між низкою інституцій ЄС, кожна з яких виконує специфічні функції у цій сфері. З метою систематизації основних організаційних компонентів цифрового суверенітету ЄС доцільно виділити їх у структурованому вигляді (табл. 2).

Таким чином, інституційна модель цифрового суверенітету в ЄС є багатокомпонентною системою, яка поєднує політичні, технічні, правові та управлінські інструменти. На відміну від американської моделі цифрової солідарності, заснованої на глобальному партнерстві, європейський підхід ґрунтується на прагненні до стратегічної автономії та контролю

Таблиця 2

Основні інституційні складові цифрового суверенітету Європейського Союзу

Інституція/Орган	Ключові функції у сфері цифрового суверенітету	Ключові ініціативи / документи
Європейська комісія	Розробка цифрової політики; законодавчі ініціативи; реалізація програм цифровізації	Цифровий компас 2030, DSA, DMA, GAIA-X
Європейський парламент	Законодавча підтримка ініціатив; контроль над виконанням цифрових стратегій	Підтримка DSA/DMA; обговорення питань кібербезпеки
Рада Європейського Союзу	Співзаконодавець; визначення стратегічних напрямів цифрового розвитку	Схвалення Цифрового компаса; позиції щодо кібербезпеки
ENISA (Агентство ЄС з кібербезпеки)	Координація кібербезпеки; створення стандартів; допомога державам-членам	Європейський акт про кіберстійкість; національні стратегії
EDPB (Європейська рада із захисту даних)	Контроль за дотриманням GDPR; захист цифрових прав громадян	Тлумачення та рекомендації щодо застосування GDPR
Національні регулятори (держави-члени)	Виконання цифрових стратегій ЄС на національному рівні; адаптація регулювання	Національні стратегії цифрової трансформації
Європейська рада з інновацій (EIC)	Фінансування інновацій, стартапів у цифровій сфері	Horizon Europe, Digital Europe Programme
Data Governance Board (DGB)	Координація використання даних у ЄС; забезпечення суверенітету даних	Data Governance Act; European Data Spaces

Джерело: власна розробка автора

над ключовими елементами цифрової екосистеми. Це зумовлено не лише прагненням до захисту економічних інтересів, а й необхідністю гарантувати інформаційну безпеку, технологічну незалежність та захист основоположних прав громадян у цифровому середовищі. У майбутньому посилення інституційного виміру цифрового суверенітету в Європі, імовірно, відіграватиме дедалі важливішу роль у формуванні нових глобальних правил цифрової гри.

Україна, перебуваючи в умовах війни та активної цифрової трансформації, стикається з низкою викликів у сфері цифрового суверенітету. Ці виклики охоплюють як внутрішні проблеми, пов'язані з нормативно-правовим забезпеченням та інституційною спроможністю, так і зовнішні загрози, зокрема кібератаки з боку держав-агресорів.

Одним із ключових викликів є відсутність цілісної та узгодженої нормативно-правової бази у сфері цифрового суверенітету. Хоча в Україні існують окремі законодавчі акти, спрямовані на регулювання інформаційної безпеки та кібербезпеки, вони часто не узгоджені між собою та не враховують сучасних викликів. Одним із ключових нормативних актів у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року, який визначає правові та організаційні основи захисту національних інтересів у кіберпросторі, а також повноваження державних органів у цій сфері [11]. У 2025 році було затверджено План заходів з реалізації Стратегії кібербезпеки України, який передбачає конкретні кроки щодо посилення кіберзахисту, включаючи створення єдиної системи реагування на кіберінциденти та впровадження посад відповідальних за кібербезпеку в органах влади та критичній інфраструктурі [12].

Крім того, в березні 2025 року Верховна Рада ухвалила Закон № 11290, який вносить зміни до законодавства щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури. Цей закон передбачає створення єдиної системи реагування на кібератаки та запровадження посад відповідальних за кібербезпеку в органах влади та критичній інфраструктурі. У сфері цифрової трансформації важливу роль відіграє Міністерство цифрової трансформації України, яке координує впровадження електронних послуг та розвиток цифрової інфраструктури. Зокрема, реалізується проект «Дія», який об'єднує низку електронних сервісів для громадян та бізнесу.

Україна постійно зазнає кібератак з боку держав-агресорів, що спрямовані на дестабілізацію інформаційного простору, порушення роботи критичної інфраструктури та викрадення конфіденційної інформації. За даними Національного координаційного центру кібербезпеки при РНБО України, у 2024 році було зафіксовано понад 3 000 кібератак на державні органи та об'єкти критичної інфраструктури [13]. Ці атаки включали як DDoS-атаки, так і складніші методи, такі як фішинг, використання шкідливого програмного забезпечення та експлуатація вразливостей у програмному забезпеченні. Особливо небезпечними є атаки на енергетичну, фінансову та транспортну інфраструктуру, які можуть мати серйозні наслідки для національної безпеки та економіки країни.

Ще одним викликом є висока залежність України від іноземних технологій, зокрема програмного забезпечення, хмарних сервісів та телекомунікаційного обладнання. Це створює ризики для цифрового суверенітету, оскільки іноземні постачальники можуть

обмежити доступ до своїх продуктів або зловживати своїм становищем. Крім того, використання іноземних технологій може призвести до витоку конфіденційної інформації та порушення національної безпеки.

Україна має значний потенціал у сфері ІТ та інновацій, проте розвиток національних технологій стримується низкою факторів, зокрема недостатнім фінансуванням, відсутністю державної підтримки та нестачею кваліфікованих кадрів. Це ускладнює створення власних технологічних рішень, які могли б замінити іноземні аналоги та забезпечити цифровий суверенітет країни.

Для подолання зазначених викликів Україна може вжити низку заходів. Зокрема, розробити та впровадити комплексну стратегію цифрового суверенітету, яка включатиме оновлення нормативно-правової бази, створення інституційної структури та визначення пріоритетних напрямів розвитку. Також важливо забезпечити зменшення залежності від іноземних технологій через підтримку національних виробників, розвиток власних технологічних рішень та створення сприятливих умов для інноваційної діяльності. Успішна реалізація цих заходів вимагатиме консолідації зусиль держави, бізнесу, наукової спільноти та громадянського суспільства. Тільки за умови спільної роботи та стратегічного підходу Україна зможе забезпечити свій цифровий суверенітет та стати повноцінним учасником глобального цифрового простору.

Висновки і перспективи подальших досліджень. У результаті проведеного дослідження було з'ясовано, що цифровий суверенітет являє собою багатогранне поняття, що поєднує технологічну незалежність держави, здатність захищати критичну цифрову інфраструктуру та здійснювати ефективне публічне управління в умовах цифрової трансформації. У контексті публічного управління цифровий суверенітет відіграє ключову роль у забезпеченні національної безпеки, збереженні інформаційного простору, а також у гарантуванні цифрових прав громадян. Аналіз інституційного наповнення цього поняття в європейському управлінському просторі дозволив виокремити низку ключових елемен-

тів, серед яких: наявність стратегічних документів цифрової трансформації, інституцій з кібербезпеки, нормативно-правова база щодо захисту даних (зокрема GDPR), а також стимулювання розвитку національних технологічних екосистем.

Оцінка стану інституційного забезпечення цифрового суверенітету в Україні показала наявність низки суттєвих викликів, серед яких: фрагментарність нормативно-правового поля, слабка координація між інституціями, висока залежність від іноземних технологій, а також недостатнє фінансування у сфері цифрової безпеки. Водночас Україна демонструє поступове наближення до європейських стандартів, зокрема шляхом створення цифрових державних сервісів, розвитку системи кіберзахисту, а також інтеграції до європейських ініціатив у сфері цифрової безпеки.

У рамках дослідження запропоновано адаптувати до українських реалій низку ефективних європейських практик. Серед них: розробка комплексної національної стратегії цифрового суверенітету, гармонізація нормативно-правового забезпечення із законодавством ЄС, створення центрів цифрової автономії, підтримка національних виробників критичних технологій та посилення міжвідомчої координації. Реалізація цих заходів сприятиме підвищенню спроможності України у сфері захисту цифрових інтересів, зменшенню зовнішніх залежностей і формуванню сталого цифрового середовища.

Перспективи подальших досліджень полягають у більш глибокому аналізі механізмів реалізації цифрового суверенітету в конкретних секторах (енергетика, транспорт, охорона здоров'я), вивченні впливу міжнародного права на формування національних цифрових політик, а також в оцінюванні ефективності вже впроваджених заходів на основі емпіричних даних. Окрему увагу варто приділити порівняльному аналізу моделей цифрового суверенітету в країнах Центрально-Східної Європи, що мають спільний історичний і політичний досвід із Україною, що дозволить адаптувати успішні інституційні рішення до національного контексту.

Література

1. Калайда Ю.П. Забезпечення цифрового суверенітету в умовах геополітичного протистояння: кращі практики зарубіжного досвіду. *Інформація і право*. 2021. Вип. 2(37). С. 145–154. URL: <http://il.ippi.org.ua/article/view/238363> (дата звернення: 01.05.2025).
2. Доронін І.М. Правові проблеми суверенізації Інтернету. *Інформація і право*. 2019. Вип. 2(29). С. 74–81. [https://doi.org/10.37750/2616-6798.2019.2\(29\).249380](https://doi.org/10.37750/2616-6798.2019.2(29).249380).
3. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. Вип. 1(32). С. 80–87. [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311).
4. Гнатюк С. Геополітичне цифрове візонерство США та ЄС: цифрова солідарність, цифровий суверенітет і нова американська стратегія розвитку міжнародного кіберпростору. 06.01.2025. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/heopolitychne-tsyfrovo-vizionerstvo-ssha-ta-yes-tsyfrova?__cf_chl_tk=SHZuM5lvNOIFrbfWqjZRhumgY7iKRGHLMf0rL_ML04-1746070327-1.0.1.1-wAB0fYGy4s5_MVR5EAZ5C2TH96jPjcGPIs11ZVK2lfQ (дата звернення: 01.05.2025).

5. Милосердна І. М. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Політикус*. 2024. Вип. 6. С. 154–160. <https://doi.org/10.24195/2414-9616.2024-6.23>.
6. Дубов Д. В. «Цифровий суверенітет» у сучасному світі: виклики та можливості для України. *Вісник Національної академії керівних кадрів культури і мистецтв*. 2015. Вип. 1. С. 205–209. URL: <https://journals.urau.ua/visnyknakkkim/article/download/138366/135286> (дата звернення: 01.05.2025).
7. Єфремова К. В. Забезпечення цифрового суверенітету держави в умовах індустрії 4.0. *Конституційні засади розвитку інноваційного суспільства: зб. наук. пр. за матеріалами інтернет-конференції* (м. Харків, 25 червня 2021 року) / за ред. А. В. Стріжкової. Харків : НДІ ПЗІР НАПрН України, 2021. С. 25–30. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/content> (дата звернення: 01.05.2025).
8. Barrinha A., Christou G. Speaking sovereignty: The EU in the cyber domain. *European Security*. 2022. Vol. 31(3) P. 356–376. <https://doi.org/10.1080/09662839.2022.2102895>.
9. Bellanova R., Carrapico H., Duez, D. Digital sovereignty and European security integration: An introduction. *European Security*. 2022. Vol. 31(3). P. 337–355. <https://doi.org/10.1080/09662839.2022.2101887>.
10. Crespi F., Caravella S., Menghini M., Salvatori Ch. European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*. 2021. Vol. 56(6). P. 348–354. URL: <https://www.intereconomics.eu/contents/year/2021/number/6/article/europeantechnological-sovereignty-an-emerging-framework-forpolicy-strategy.html> (дата звернення: 01.05.2025).
11. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII від 5 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 01.05.2025).
12. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 7 березня 2025 р. № 204-р. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80>. (дата звернення: 01.05.2025).
13. Казанцев Д. Кібербезпека під час війни: виклики, тренди, стартапи. *Українська правда*. 20.03.2025. URL: <https://mezha.media/articles/vid-diversiy-do-shpigunstva-vikliki-ta-trendi-kiberviyni-300559/amp/> (дата звернення: 01.05.2025).

References

1. Kalaida, Yu. P. (2021). Zabezpechennia tsyfrovoho suverenitetu v umovakh heopolitychnoho protyborstva: krashchi praktyky zarubizhnogo dosvidu [Ensuring digital sovereignty under geopolitical confrontation: Best foreign practices]. *Informatsiia i pravo — Information and Law*, (2)37, 145–154. <http://il.ippi.org.ua/article/view/238363> [in Ukrainian].
2. Doronin, I. M. (2019). Pravovi problemy suverenizatsii Internetu [Legal problems of Internet sovereignization]. *Informatsiia i pravo — Information and Law*, (2)29, 74–81. [https://doi.org/10.37750/2616-6798.2019.2\(29\).249380](https://doi.org/10.37750/2616-6798.2019.2(29).249380) [in Ukrainian].
3. Solodka, O. M. (2020). Zabezpechennia informatsiinoho suverenitetu derzhavy: pravovyi dyskurs [Ensuring state information sovereignty: Legal discourse]. *Informatsiia i pravo — Information and Law*, (1)32, 80–87. [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311) [in Ukrainian].
4. Hnatiuk, S. (2025, January 6). Heopolitychne tsyfrovoe viziunerstvo SSHA ta YeS: tsyfrova solidarist, tsyfrovyy suverenitet i nova amerykanska stratehiia rozvytku mizhnarodnoho kiberprostoru [Geopolitical digital vision of the USA and EU: Digital solidarity, digital sovereignty, and the new American strategy for international cyberspace development]. <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/heopolitychne-tyfrove-vizionerstvo-ssha-ta-yes-tyfrova> [in Ukrainian].
5. Myloserdna, I. M. (2024). Tsyfrovyy suverenitet derzhavy: naukova rytoryka ta realni zminy [State digital sovereignty: Scientific rhetoric and real changes]. *Politykus — Politykus Academic Journal*, (6), 154–160. <https://doi.org/10.24195/2414-9616.2024-6.23> [in Ukrainian].
6. Dubov, D. V. (2015). «Tsyfrovyy suverenitet» u suchasnomu sviti: vyklyky ta mozhlyvosti dlia Ukrainy [«Digital sovereignty» in the modern world: Challenges and opportunities for Ukraine]. *Visnyk Natsionalnoi akademii kerivnykh kadrov kultury i mystetstv — Bulletin of the National Academy of Culture and Arts Leadership*, (1), 205–209. <https://journals.urau.ua/visnyknakkkim/article/download/138366/135286> [in Ukrainian].
7. Yefremova, K. V. (2021). Zabezpechennia tsyfrovoho suverenitetu derzhavy v umovakh industrii 4.0 [Ensuring digital sovereignty of the state under Industry 4.0]. In A. V. Strizhkova (Ed.), *Konstitutsiini zasady rozvytku innovatsiinoho suspilstva — Constitutional Principles of Innovation Society Development* (pp. 25–30). Kharkiv: NDI PZIR NAPrN Ukrainy. <https://openarchive.nure.ua/server/api/core/bitstreams/f981db39-23a5-470f-bf25-e1af2f3701dc/content> [in Ukrainian].
8. Barrinha, A., & Christou, G. (2022). Speaking sovereignty: The EU in the cyber domain. *European Security*, 31(3), 356–376. <https://doi.org/10.1080/09662839.2022.2102895> [in English].
9. Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital sovereignty and European security integration: An introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887> [in English].
10. Crespi, F., Caravella, S., Menghini, M., & Salvatori, Ch. (2021). European technological sovereignty: An emerging framework for policy strategy. *Intereconomics*, 56(6), 348–354. <https://www.intereconomics.eu/contents/year/2021/number/6/article/europeantechnological-sovereignty-an-emerging-framework-forpolicy-strategy.html> [in English].

11. Verkhovna Rada Ukrainy. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 2163-VIII vid 5 zhovtnia 2017 roku* [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017]. <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].

12. Kabinet Ministriv Ukrainy. (2025). *Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy: Rozporiadzhennia KМУ vid 7 bereznia 2025 r. № 204-r* [On approval of the 2025 action plan for implementing the Cybersecurity Strategy of Ukraine: Order of the CMU No. 204-r dated March 7, 2025]. <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80> [in Ukrainian].

13. Kazantsev, D. (2025, March 20). Kiberbezpeka pid chas viiny: vyklyky, trendy, startapy [Cybersecurity during war: Challenges, trends, startups]. *Ukrainska Pravda — Ukrainian Truth*. <https://mezha.media/articles/vid-diversiy-doshpigunstva-vikliki-ta-trendi-kiberviyni-300559/amp/> [in Ukrainian].

Стаття надійшла до редакції 06.05.2025