УДК 339.923:004(4-6ЄС)
DOI: https://doi.org/10.32782/2415-8801/2026-2.2

Бочарова Ю.Г.
доктор економічних наук, професор,
професор кафедри технологій в ресторанному господарстві,
готельно-ресторанної справи та менеджменту,
Криворізький національний університет
ORCID: https://orcid.org/0000-0002-4829-8948

Чернега О.Б.
доктор економічних наук, професор,
професор кафедри технологій в ресторанному господарстві,
готельно-ресторанної справи та менеджменту,
Криворізький національний університет
ORCID: https://orcid.org/0000-0002-8504-6299

Кожухова Т.В.
доктор економічних наук, професор,
професор кафедри технологій в ресторанному господарстві,
готельно-ресторанної справи та менеджменту,
Криворізький національний університет
ORCID: https://orcid.org/0000-0001-6758-9890

ЦИФРОВА БЕЗПЕКА ЄС: АНАЛІЗ БЕЗПЕКОВИХ ДЕФІЦИТІВ ТА ОЦІНКА ЦИФРОВОЇ РЕЗИЛЬЄНТНОСТІ[1]

У статті здійснено комплексну оцінку поточного рівня цифрової безпеки Європейського Союзу через призму реалізації стратегії «Цифрового десятиліття 2030». Установлено, що на стику програмних періодів 2019–2024 та 2024–2029 років цифрова трансформація в ЄС перетворилася на наскрізний інструмент гарантування стратегічної автономії та безпеки. На основі аналізу звітів про стан Цифрового десятиліття за 2023–2026 роки виявлено глибоку міжсекторальну асиметрію цифрового розвитку ЄС. Установлено, що незважаючи на активний розвиток сектору цифрових державних послуг (середній рівень виконання цілей досяг 87,5%), в архітектурі технологічного суверенітету ЄС зберігаються критичні зони безпекового дефіциту. Найбільш загрозливими трендами визначено регрес у досягненні цілі у сфері виробництва напівпровідників (дефіцит становить 56 в.п.) та системне відставання у впровадженні штучного інтелекту підприємствами (дефіцит становить 73 в.п.). Запропоновано якісну характеристику безпекових дефіцитів здійснювати на основі їх ролі у забезпеченні цифрової безпеки, що дозволило ідентифікувати операційні, структурні та критичні дефіцити цифрової безпеки ЄС. Доведено, що поточна модель цифрового розвитку ЄС тяжіє до «інфраструктурно-сервісного» типу, що формує хронічну імпортозалежність від апаратного забезпечення з третіх країн. Обґрунтовано, що подолання виявлених дефіцитів є базовою умовою забезпечення цифрової резильєнтності критичної інфраструктури ЄС.

Ключові слова: *цифровізації економіки та суспільства, цифрова трансформація, цифрова безпека, ЄС, безпековий дефіцит, цифрова резильєнтність, технологічний суверенітет.*

[1] Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project: 101127413 – EVSDESCI – ERASMUS-JMO-2023-HEI-TCH-RSCH

EU DIGITAL SECURITY: ANALYSIS OF SECURITY DEFICITS AND ASSESSMENT OF DIGITAL RESILIENCE

Bocharova Yuliia, Chernega Oksana, Kozhukhova Tetiana
Kryvyi Rih National University

In the context of global geopolitical shifts and rapid technological progress, digital security and technological sovereignty have become pivotal elements of national and regional stability. At the intersection of the 2019–2024 and 2024–2029 programming periods, the European Union has increasingly integrated digital transformation as a cross-cutting instrument to guarantee its strategic autonomy. However, the practical implementation of these ambitions faces significant challenges. Assessing the actual progress of the EU towards its digital goals is crucial for understanding its vulnerability to external shocks and identifying structural gaps in its security. The purpose of this article is to conduct a comprehensive assessment of the current level of digital security in the European Union by analyzing progress and identifying disparities in achieving the strategic goals of the "Digital Decade 2030" through the prism of key security and technological determinants. Based on an in-depth analysis of the State of the Digital Decade reports for 2023–2026, a profound cross-sectoral asymmetry in the EU's digital development was revealed. It is established that while the digital public services sector demonstrates exemplary progress (with the average target achievement rate reaching 87.5%), critical zones of security deficits persist in the architecture of the EU's technological sovereignty. The most threatening trends identified include a regression in semiconductor manufacturing, where the target deficit stands at 56 percentage points (p.p.), and a systemic lag in the adoption of artificial intelligence by enterprises, showing a deficit of 73 p.p. To address these gaps, a qualitative classification of security deficits is proposed based on their role in ensuring digital security: critical deficits (directly determining digital sovereignty); structural deficits (shaping the long-term capacity of the economy to create, implement, and scale digital technologies); and operational deficits (affecting the efficiency of digital transformations without directly determining the level of digital sovereignty). The study proves that the current model of the EU's digital development heavily gravitates toward an «infrastructure-and-service» type, which fosters chronic import dependence on hardware from third countries. The research concludes that the identified security deficits pose a significant threat to the EU's geopolitical standing and economic security. Overcoming these critical, structural, and operational deficits is a fundamental prerequisite for ensuring the digital resilience of the EU's critical infrastructure. To achieve genuine strategic autonomy, the EU must transition from its current model to a robust, self-sufficient technological framework by actively bridging the gaps in hardware manufacturing and advanced technology adoption.

Keywords: *digitization of economy and society, digital transformation, digital security, EU, security deficit, digital resilience, technological sovereignty.*

Постановка проблеми. У сучасних умовах геополітичної нестабільності, ескалації технологічної конкуренції та зростання масштабів кіберзагроз, цифрова безпека Європейського Союзу трансформується із суто технічного завдання захисту інформаційних систем у фундаментальний базис його стратегічної автономії та економічної стійкості. Така трансформація знаходить прояв у зміні політичної парадигми Європейської Комісії на стику програмних періодів (2019–2024 рр., 2024–2029 рр.), внаслідок якої цифрова трансформація переросла рамки окремої цілі та перетворилася на наскрізний «горизонтальний» інструмент гарантування економічної безпеки, чистої промисловості та конкурентоспроможності [1]. Масштабні інвестиційні вливання, зокрема через Механізм відновлення та стійкості, спрямовані на забезпечення макроекономічної ефективності цифровізації та генерацію мультиплікативного ефекту (мультиплікатор ЄС становить 1,5) [2], проте реалізація цього потенціалу стримується структурними диспропорціями. Операціоналізація зазначеного курсу в межах глобальної стратегії «Цифрового десятиліття 2030» через модель «Цифрового компаса» потребує нових методологічних підходів до моніторингу. Забезпечення цифрової безпеки сьогодні не може оцінюватися відірвано від темпів досягнення цільових орієнтирів за чотирма базовими блоками компаса (навичками, інфраструктурою, бізнесом та держпослугами), а також поза контекстом дотримання фундаментальних прав і розвитку міжнародних партнерств [3]. Без такого підходу неможливо чітко ідентифікувати приховані зони безпекового дефіциту, що послаблюють загальну систему цифрової резильєнтності та технологічного суверенітету ЄС.

Аналіз останніх досліджень і публікацій. Питання інфраструктурного забезпечення цифрової трансформації, безпеки критичних технологій досліджували багато як зарубіжних, так і укра-

їнських учених. Водночас, попри глибокий аналіз загальних трендів цифровізації, поза увагою дослідників часто залишається кількісна оцінка дефіцитів виконання цільових орієнтирів «Цифрового десятиліття 2030» саме в контексті формування стратегічної безпекової автономії ЄС.

Питання формування безпекової архітектури та забезпечення цифрового суверенітету ЄС і України у своїх працях детально досліджує Ю. Калюжна[4]. Авторка розуміє цифровий суверенітет не просто як контроль над активами, а як здатність держави чи інтегрованого регіону самостійно визначати цифрову політику та захищати критичну інфраструктуру в парадигмі «суверенітету над цифровим» та «суверенітету через цифрове» [4]. У її дослідженні особливу увагу приділено еволюції регуляторного поля ЄС – від «Цифрового порядку денного для Європи» до стратегічних цілей програми «Цифрового компаса 2030», а також аналізу ключових наднаціональних актів (GDPR, Cyber Security Act, AI Act тощо), що виступають інструментами мінімізації транскордонних гібридних загроз та захисту цифрових прав громадян [4]. Проте, попри високу теоретичну цінність цих напрацювань, поза увагою дослідниці залишився прикладний макроекономічний інструментарій оцінювання зон безпекового дефіциту через відносні показники виконання цільових показників, визначених у межах чотирьох базових цільових блоків параметрів Цифрового десятиліття.

Череп А.В., Воронкова В.Г. приходять до висновку, що «цифрова безпека в європейській економіці – це сукупність заходів, політик та технологій, спрямованих на захист цифрової інфраструктури, персональних даних, фінансових систем та промислових мереж від кіберзагроз, збоїв і несанкціонованого доступу» [5].

Концептуальні засади формування цифрового суверенітету як інструменту протидії нестабільності в Європі детально досліджено у праці С. Ананда, Ш. Доннеллі, М. Еренхарда, Л. Ньювенхейса та А. Абхішти. Автори спрямовують свій аналіз на концептуалізацію суверенітету в кіберпросторі як відповідь на цифрову нестабільність в Європі в умовах зростання геополітичної напруженості. Наукова новизна їхньої праці полягає у застосуванні якісної методології Джойя (Gioia methodology) для критичного аналізу 79 відібраних правових документів ЄС, що дозволило авторам ідентифікувати шість ключових вимірів стратегічних та цифрових цілей Євросоюзу, обґрунтувати їхній зв'язок із цифровою безпекою, а головне – на основі емпіричних даних наочно виявити та підкреслити прогалини в їхній практичній імплементації. Зазначене дослідження частково перегукується з теоретичними розвідками Ю. Калюжної, проте суттєво відрізняється суворим фокусом на емпіричному кодуванні законодавчих актів та пошуку інституційних розривів усередині нормативного поля ЄС [6].

Продовженням та логічним доповненням аналізу інституційних і нормативних бар'єрів у межах забезпечення цифрової безпеки ЄС є праця М. Рожер, Е. Лопеса та С. Мартіна, які концентрують увагу на комплексному дослідженні практичних викликів та потенційних можливостей реалізації цифрового суверенітету в Європейському Союзі [7]. Автори детально розглядають дуалістичну природу цього процесу, обґрунтовуючи, що з одного боку, формування стратегічної автономії гальмується через критичну залежність від іноземних технологічних рішень та фрагментарність ринку, а з іншого – успішна розбудова цифрового суверенітету відкриває значні можливості для стимулювання внутрішніх європейських інновацій та захисту екосистеми критичних технологій [7]. Проте, попри глибоке структурування якісних факторів впливу та макроекономічних викликів, у зазначеному дослідженні, як і в попередніх працях, поза увагою залишається прикладний математичний інструментарій кількісного вимірювання дефіцитів у виконанні індикативних траєкторій програми «Цифрового компаса 2030».

Постановка завдання. Метою статті є комплексна оцінка поточного рівня цифрової безпеки Європейського Союзу шляхом аналізу прогресу та виявлення диспропорцій у досягненні стратегічних цілей «Цифрового десятиліття 2030» у розрізі ключових безпеково-технологічних детермінант.

Виклад основного матеріалу дослідження. З огляду на багатовекторну архітектуру «Цифрового компаса», оцінку рівня цифрової безпеки та стратегічної автономії доцільно проводити не через абсолютні значення індикаторів, а через інтегральний аналіз відсотків виконання встановлених на 2030 рік цілей для кожного з чотирьох визначених блоків. Такий підхід дозволить чітко ідентифікувати зони безпекового дефіциту за конкретними стратегічними напрямами (табл. 1).

Аналіз звітів Report on the state of the Digital Decade за 2023–2026 рр.[2] свідчить, що протягом зазначеного періоду цифрова трансформація в ЄС набула системного, однак виражено асиметричного та диспропорційного характеру.

Найбільш успішно у 2023–2026 рр. відбувалася розбудова цифрової інфраструктури. Так, протягом усього періоду усереднений рівень виконання цілей групи показників розвитку цифрової інфраструктури збільшився на 33,7 в.п. (для порівняння: усереднене значення групи показників цифрової трансформації бізнесу зросло на 16,8 в.п., цифрових навичок – на 6,4 в.п., цифровізації державних послуг – на 9,75 в.п.). Попри те, що цифрова інфраструктура розвивалася найвищими

Таблиця 1

Прогрес у досягненні цілей Digital Decade

Показники	Цільове значення	Досягнуті значення, % виконання цілі				Відхилення		Безпековий дефіцит[7]
	Роки							
	2030	2023	2024	2025	2026	2023–2026	2026–2030	2026
Цифрова інфраструктура								
Покриття 5G	100%	81	89	94	97	16	-3	операційний
Покриття 5G на 3,4–3,8 ГГц	100%	41	51	67,7	75	34	-25	операційний
Оптоволоконне підключення	100%	56	64	69,2	74	18	-26	операційний
Фіксований інтернет	100%	75	79	82,5	86	11	-14	операційний
Напівпровідники	<2 нм, 20%[1]	50	55	53	44	-6	-56	критичний
Периферійні вузли обробки даних	10000	12	12	23	75	63	-25	структурний
Квантові комп'ютери	3 шт.	0	33	67	100	100	0	–
Середній рівень виконання цілей групи		45	54,7143	65,2	78,7	33,7	-21,3	не визначено
Цифрова трансформація бізнесу								
Суб'єкти МСП із щонайменше базовим рівнем цифрової інтенсивності	90%[2]	77	64	81	79	2	-21	операційний
Хмарні технології	75%[3]	45	52	52	62	17	-38	структурний
Великі дані	75%[3]	19	44	44	53	34	-47	структурний
Штучний інтелект	75%[3]	11	11	18	27	16	-73	критичний
Компанії-єдинороги	498 шт.	50	53	57	65	15	-35	структурний
Середній рівень виконання цілей групи		40,4	44,8	50,4	57,2	16,8	-42,8	не визначено
Цифрові навички								
Базові цифрові навички	80%[4]	68	69	70	75	7	-25	структурний
ІТ-спеціалісти	20[5]	47	48	52	52,85	5,85	-47,2	структурний
Середній рівень виконання цілей групи		57,5	58,5	61	63,9	6,4	-36,1	не визначено
Цифрові державні послуги								
Послуги для громадян	100	77	79	82,3	85	8	-15	операційний
Послуги для бізнесу	100	84	85	86,2	89	5	-11	операційний
Електронне здоров'я	100	72	79	82,7	87	15	-13	операційний
Електронна ідентифікація	27[6]	78	85	89	89	11	-11	операційний
Середній рівень виконання цілей групи		77,75	82	85,05	87,5	9,75	-12,5	не визначено

1 – світового виробництва; 2 – малих та середніх підприємств (МСП); 3 – підприємств; 4 – осіб; 5 – млн зайнятих; 6 – країн з електронною ідентифікацією; 7 – якісна характеристика безпекових дефіцитів, що базується на їх ролі у забезпеченні цифрової безпеки: критичні дефіцити – безпосередньо визначають цифровий суверенітет; структурні дефіцити – формують довгострокову спроможність економіки створювати, впроваджувати та масштабувати цифрові технології; операційні дефіцити – впливають на ефективність цифрових перетворень, але не визначають безпосередньо рівень цифрового суверенітету.

Джерело: складено та розраховано автором на основі даних [2]

темпами, мінімальне усереднене відставання від цільових орієнтирів 2030 року зафіксовано в секторі цифровізації державних послуг – у середньому 12,5 в.п. (для порівняння: дефіцит виконання планових показників за напрямом цифрової інфраструктури становив 21,3 в.п., цифрової трансформації бізнесу – 42,8 в.п., цифрових навичок – 36,1 в.п.).

Крім того, у 2023–2026 рр. найвищу динаміку продемонстрували окремі компоненти цифрової інфраструктури. Зокрема, у 2026 році в ЄС зафіксовано стовідсоткове виконання цілі щодо розгортання квантових комп'ютерів (приріст прогресу на 100 в.п. порівняно з 2023 роком). Стрімке прискорення відбулося також у сегменті периферійних вузлів обробки даних, де рівень виконання цілі зріс із критичних 12% до 75% (+63 в.п.). Водночас базове покриття 5G майже досягло цільового значення (97% виконання цілі), тоді як стратегічно важливі напрями – розгортання високочастотного 5G (3,4–3,8 ГГц) та оптоволоконного підключення – демонструють суттєве відставання від плану (план виконано лише на 75% та 74% відповідно).

Найбільш проблемним трендом є регрес у досягненні стратегічної цілі щодо частки ЄС у світовому виробництві напівпровідників. Рівень досягнення цілі (забезпечення 20% світового ринку мікросхем) після короткочасного зростання у 2024 році (до 55%) упав до 44% у 2026 році. Це означає, що ЄС ризикує не наздогнати світових лідерів, а дефіцит виконання плану до 2030 року наразі становить найбільші серед інфраструктурних проєктів 56 в.п.

У сфері трансформації бізнесу та навичок спостерігається інертність. Прогрес у впровадженні штучного інтелекту підприємствами становить лише 27% від цільового показника, відповідно дефіцит виконання у 73 в.п. Схожа ситуація і з підготовкою IT-спеціалістів: за три роки рівень виконання цілі збільшився усього на 5,85 в.п. (до 52,85%), що свідчить про серйозний дефіцит кадрів на ринку.

Натомість найменш асиметричним та найбільш прогнозованим є сектор цифрових державних послуг. Усі без винятку показники (послуги для громадян, бізнесу, e-Health та eID) демонструють стабільне зростання, а рівень їхнього виконання у 2026 році коливається в межах 85–89%. Відповідно, відставання від цільових показників 2030 року тут є мінімальним (від 11 до 15 в.п.), що робить цей напрям лідером за якістю та збалансованістю європейського цифрового треку.

Отримані результати розрахунків свідчать, що найбільше невиконання цілей фіксується у таких критичних точках технологічного суверенітету – сегменті штучного інтелекту та мікроелектроніки (напівпровідників). З позицій цифрової безпеки це означає, що попри зразкову цифровізацію державних послуг (де дефіцит становить лише 11–15 в.п.), ЄС залишається залежним від зовнішніх постачальників апаратного забезпечення та відстає у сфері суверенних оборонних та аналітичних алгоритмів. Таким чином, асиметрія європейського цифрового треку створює додаткові ризики для безпеки критичної інфраструктури в умовах ескалації гібридних загроз.

Глибока міжсекторальна диспропорційність, виявлена під час аналізу, актуалізує питання ефективності поточних інструментів фінансування ЄС, зокрема Механізму відновлення та стійкості (RRF). Попри нормативну вимогу щодо обов'язкового спрямування щонайменше 20% коштів національних планів відновлення (RRP) на потреби цифровізації [8], реальний розподіл цього капіталу виявив суттєві структурні дисбаланси.

Наднаціональні фінансові ін'єкції здебільшого абсорбуються секторами з коротким інвестиційним циклом та гарантованою капіталовіддачею, такими як цифровізація публічних сервісів. Сектор Цифрових державних послуг продемонстрував високу адаптивність завдяки наявності сильних централізованих регуляторних інституцій та відносній простоті масштабування програмного забезпечення.

Натомість капіталомісткі високотехнологічні напрями з тривалим періодом окупності демонструють системне гальмування. Падіння рівня виконання цілі по напівпровідниках до 44% у 2026 році яскраво демонструє, що ухвалений у 2023 році Європейський акт про мікросхеми (EU Chips Act) [9] наразі стикається із жорстким глобальним супротивом та хронічним браком приватного венчурного капіталу в ЄС. Будівництво передових фаундрі-заводів (заводи, що виготовляють мікросхеми та напівпровідники за проєктами інших компаній) вимагає тривалого часу, тоді як геополітична нестабільність та асиметрія субсидування мікроелектроніки у США та Азії послаблюють конкурентні позиції Євросоюзу.

Окремим критичним бар'єром для безпеки є критична інертність у сферах трансформації бізнесу та цифрових навичок. Дефіцит у 73 в.п. у розгортанні штучного інтелекту є прямим наслідком дії двох чинників:

Регуляторного тиску нового Акта про ШІ, який, хоч і спрямований на мінімізацію ризиків кібербезпеки, водночас може створювати додаткові витрати, що дестимулюють малий та середній бізнес (МСП) до експериментів із проривними технологіями через загрозу високих штрафів [10].

Гострого кадрового дефіциту – низький приріст частки IT-фахівців (+5,85 в.п. за 3 роки) створює бар'єри для технологічного переоснащення компаній. Без наявності кваліфікованих кадрів навіть за умови повного інфраструктурного забезпечення (наприклад, 100% покриття 5G чи наявності квантових комп'ютерів) бізнес та сектор оборони неспроможні ефективно інтегрувати складні аналітичні алгоритми.

Таким чином, європейська модель цифрового розвитку наразі тяжіє до «інфраструктурно-сервісного» типу, що характеризується високою імпортозалежністю від іноземних хмарних обчислень, систем великих даних та мікросхем, незважаючи на значні успіхи у розвитку цифрової інфраструктури та е-урядування.

Висновки з проведеного дослідження. Проведена комплексна оцінка прогресу досягнення цілей Digital Decade за період 2023–2026 рр. підтвердила тезу про глибоку структурну асиметрію цифрового треку ЄС. Встановлено, що цифрова інфраструктура розвивається найвищими темпами (+33,7 в.п. виконання плану групи), тоді як розбудова людського капіталу та цифрових навичок демонструє максимальну інертність (+6,4 в.п.), що формує ключове обмеження для загальної ефективності інвестицій.

Виявлено критичні точки безпекового дефіциту в архітектурі технологічного суверенітету ЄС. Найбільш загрозливим трендом визначено регрес у сфері виробництва напівпровідників (дефіцит до цілі становить 56 в.п.) та критичне відставання у впровадженні штучного інтелекту (зазор невиконання – 73 в.п.). Це свідчить про те, що ЄС залишається вразливим перед зовнішніми геоекономічними шоками та залежним від апаратних рішень третіх країн.

Доведено, що найбільш збалансованим та інституційно захищеним вектором є сектор цифрових державних послуг (середній рівень виконання цілей досяг 87,5% у 2026 році). Електронне урядування та цифрова ідентифікація виступають стабілізаційним ядром цифрової системи ЄС, проте їхня стійкість у довгостроковій перспективі прямо залежатиме від подолання критичних безпекових дефіцитів у hardware-сегменті інфраструктури.

Подальші дослідження у цьому напрямі будуть спрямовані на розробку економетричних моделей, що дозволять кількісно оцінити вплив міжсекторальних цифрових дефіцитів на інтегральний індекс національної безпеки окремих країн-членів ЄС, а також на обґрунтування адаптивних механізмів фінансування цифрової резильєнтності в умовах мінливого геополітичного ландшафту.

Список використаних джерел:

1. European Commission Strategic Priorities / European Commission. URL: https://commission.europa.eu/strategy-and-policy/.

2. Reports on the State of the Digital Decade (2023–2026) / European Commission. Digital Decade Reports. URL: https://digital-strategy.ec.europa.eu/en/library.

3. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions 2030 Digital Compass: the European way for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021 DC0118.

4. Калюжна Ю.І. Цифровий суверенітет як фактор національної безпеки ЄС та України. URL: https://www.researchgate.net/publication/393363261_Cifrovij_suverenitet_ak_faktor_nacionalnoi_bezpeki_ES_ta_Ukraini.

5. Socio-economic security in the context of war: innovative approaches and strategic guidelines for the postwar period : collective monograph / edited by A. V. Cherep, I. M. Dashko, Yu. O. Ohrenych, O. H. Cherep. Riga, Latvia : Baltija Publishing, 2025. 218 p.

6. Anand S., Donnelly S., Ehrenhard M., Nieuwenhuis L. J. M., & Abhishta A. (2026). Digital sovereignty and the means to European digital security: identification of the goals related to digital sovereignty from legal texts published by the European Union. European Security. URL: https://doi.org/10.1080/ 09662839.2026.2627905

7. Maribel R., Lopez E., Martin C. Digital Sovereignty in the European Union: Challenges and Opportunities. 2025. DOI: https://doi.org/10.13140/RG.2.2. 22387.85281.

8. Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. URL: https://eur-lex.europa.eu/eli/reg/2021/241/oj.

9. European Chips Act. URL: https://digital-strategy.ec.europa.eu/en/policies/ european-chips-act.

10. The EU Artificial Intelligence Act. URL: https://artificialintelligenceact.eu/.

References:

1. European Commission. (2024). European Commission Strategic Priorities. Available at: https://commission.europa.eu/strategy-and-policy/ (accessed 17 July 2026).

2. European Commission. (2026). Reports on the State of the Digital Decade (2023–2026). Digital Decade Reports. Available at: https://digital-strategy.ec.europa.eu/en/library (accessed 17 July 2026).

3. European Commission. (2021). Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions 2030 Digital Compass: the European way for the Digital Decade. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed 17 July 2026).

4. Kaliuzhna Yu.I. (2026). Tsyfrovii suverenitet yak faktor natsionalnoi bezpeky YeS ta Ukrainy [Digital sovereignty as a factor of national security of the EU and Ukraine]. ResearchGate. Available at: https://www.researchgate.net/publication/393363261_Cifrovij_suverenitet_ak_faktor_nacionalnoi_bezpeki_ES_ta_Ukraini [in Ukrainian]

5. Cherep A.V., Dashko I.M., Ohrenych Yu.O., Cherep O.H. (Eds.). (2025). Socio-economic security in the context of war: innovative approaches and strategic guidelines for the postwar period. Riga, Latvia : Baltija Publishing.

6. Anand S., Donnelly S., Ehrenhard M., Nieuwenhuis L.J.M., Abhishta A. (2026). Digital sovereignty and the means to European digital security: identification of the goals related to digital sovereignty from legal texts published by the European Union. European Security. DOI: https://doi.org/10.1080/09662839.2026.2627905 (accessed 17 July 2026).

7. Maribel R., Lopez E., Martin C. (2025). Digital Sovereignty in the European Union: Challenges and Opportunities. DOI: https://doi.org/10.13140/RG.2.2.22387.85281 (accessed 17 July 2026).

8. European Parliament, Council of the European Union. (2021). Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. Available at: https://eur-lex.europa.eu/eli/reg/2021/241/oj (accessed 17 July 2026).

9. European Commission. (2023). European Chips Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-chips-act (accessed 17 July 2026).
10. European Parliament, Council of the European Union. (2024). The EU Artificial Intelligence Act. Available at: https://artificialintelligenceact.eu/ (accessed 17 July 2026).

E-mail: bocharova@donnuet.edu.ua
E-mail: chernega@donnuet.edu.ua
E-mail: kozhuhova@donnuet.edu.ua

Дата надходження статті: 12.07.2026
Дата прийняття статті до публікації: 13.08.2026
Дата публікації статті: 21.08.2026