

УДК: 327:004.738.5:321.01

DOI: 10.60022/3(4)-23S

Андрєєва Ольга Миколаївна

доктор політичних наук, професор

професор кафедри міжнародної інформації

Навчально-науковий інститут міжнародних відносин

Київський національний університет імені Тараса Шевченка, Україна

Andriieva Olha

Doctor of Political Sciences, Professor

Professor of International Information Department

Educational and Scientific Institute of International Relations

Taras Shevchenko National University of Kyiv, Ukraine

ORCID: 0000-0003-4587-1267

НЕО-ТЕХНОСУВЕРЕНІТЕТ В ГЛОБАЛІЗОВАНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРИ: МІЖ ЦИФРОВИМ АВТОРИТАРИЗМОМ І ЦИФРОВОЮ ДЕМОКРАТІЄЮ

Анотація. У статті здійснено комплексний теоретико-емпіричний аналіз феномену нео-техносуверенітету як постнекласичної форми трансформації державної влади в умовах цифровізації, глобалізації та платформізації політичного простору XXI століття. Обґрунтовано, що нео-техносуверенітет формується на перетині двох альтернативних траєкторій розвитку цифрових політичних режимів, цифрового авторитаризму та цифрової демократії, виступаючи водночас інструментом захисту автономії держави і потенційним механізмом концентрації технологічної влади.

Особливу увагу приділено українському кейсу як унікальній емпіричній лабораторії нео-техносуверенітету в умовах повномасштабної війни. Доведено, що досвід України демонструє функціональний характер сучасного суверенітету, який реалізується через стійкість цифрової держави, кібербезпеку, управління інформаційним простором і мережеву взаємодію державних, приватних та міжнародних акторів. Зроблено висновок, що нео-техносуверенітет не є нормативно нейтральним явищем, а його демократичний або авторитарний потенціал визначається рівнем громадянського контролю та прозорістю цифрового врядування.

Ключові слова: електронне урядування, національна безпека, глобалізація, міжнародні відносини та комунікація, цифровий суверенітет, big data, інформаційна безпека, гібридна війна, Україна.

NEO-TECHNOSOVEREIGNTY IN THE GLOBALIZED INFORMATION SPACE: BETWEEN DIGITAL AUTHORITARIANISM AND DIGITAL DEMOCRACY

Abstract. This article provides a comprehensive theoretical and empirical analysis of neo-technosovereignty as a post-nonclassical form of state power transformation under the conditions of digitalization, globalization, and the platformization of the political space in the twenty-first century. It is argued that neo-technosovereignty emerges at the intersection of two alternative trajectories of digital political regimes, digital authoritarianism and digital democracy, functioning simultaneously as a mechanism for safeguarding state autonomy and as a potential instrument for the concentration of technological power.

Unlike classical Westphalian idea, which was based on territorial control and the monopoly on the legitimate use of violence, neo-technosovereignty is centered on control over critical digital infrastructure, data flows, algorithms, and technological standards. The article analyzes key international theoretical approaches to digital and technological sovereignty and outlines the contributions of Ukrainian scholars, for whom technosovereignty is closely linked to issues of national security, hybrid threats, and warfare.

Special attention is devoted to the Ukrainian case as a unique empirical laboratory of neo-technosovereignty under conditions of full-scale war. It is demonstrated that Ukraine's experience reveals the



functional nature of contemporary sovereignty, which is exercised through the resilience of the digital state, cybersecurity, information space governance, and networked interaction among state, private, and international actors. The article concludes that neo-technosovereignty is not a normatively neutral phenomenon; rather, its democratic or authoritarian potential is determined by the level of civic oversight and the transparency of digital governance.

Keywords: *e-government; national security; globalization; international relations and communication; digital sovereignty; big data; information security; hybrid warfare; Ukraine.*

Постановка проблеми. У XXI столітті поняття суверенітету держави зазнає ключових фундаментальних змін під впливом цифрових технологій, глобальних інформаційних мереж і транснаціональних корпорацій. Традиційна модель державної влади, заснована на контролі над територією та населенням, поступово доповнюється, а іноді й підривається новими формами технологічної автономії та автоматизованого управління, тут формується так звана концепція нео-техносудверенітету, що визначається здатністю суб'єктів (державних і недержавних) контролювати критичні технології, цифрову інфраструктуру і дані, що стають ключовими чинниками влади, безпеки й економічного добробуту в державі.

У сучасному політичному дискурсі концепт нео-техносудверенітету формується як відповідь держав на глибоку трансформацію влади, спричинену цифровізацією, глобалізацією та зростанням ролі технологічних корпорацій. На відміну від класичного суверенітету, який ґрунтувався на територіальному контролі, монополії на легітимне насильство та юридичній автономії, нео-техносудверенітет зосереджується на здатності держави контролювати критичні цифрові інфраструктури, дані, алгоритми та технологічні стандарти, тут йдеться не лише про політичну незалежність, а про спроможність діяти незалежно в цифровому середовищі, де кордони є умовними, а влада розподілена між державами, техно-медіа-корпораціями та наднаціональними платформами.

Аналіз останніх досліджень і публікацій. Зарубіжна теорія нео-техносудверенітету бере свій початок у критичному переосмисленні класичних теорій суверенітету. Ще наприкінці XX століття дослідники звернули увагу на те, що глобалізація, транснаціональні корпорації та інформаційні технології підривають монополію держави на владу [1. 2]. У цифрову епоху ці процеси набули нового виміру, оскільки контроль над інформаційними потоками та цифровими інфраструктурами став стратегічним ресурсом.

М. Кастельс у своїй концепції «мережевого суспільства» наголошував, що влада дедалі більше реалізується через контроль над мережами та потоками інформації, а не через територіальне панування [3]. Хоча Кастельс безпосередньо не використовує термін «техносудверенітет», його теорія створює методологічне підґрунтя для розуміння суверенітету як мережевої та функціональної категорії.

У 2010-х роках у європейському та північноамериканському дискурсі з'являється поняття цифровий суверенітет, яке спочатку використовується у політичних документах ЄС, а згодом і у наукових дослідженнях. П. Поле та Т. Тіль визначають цифровий суверенітет як здатність політичних спільнот самостійно ухвалювати рішення щодо цифрових технологій та їх регулювання [4]. Важливо, що автори підкреслюють: цифровий суверенітет не означає ізоляції, а радше спроможність діяти автономно в умовах глобальної взаємозалежності. Подібний підхід розвиває і Ф. Шарпф, який аналізує втрату державами «керованості» внаслідок технологічної глобалізації та зростання ролі приватних акторів [5]. У цьому контексті техносудверенітет постає як відповідь на дефіцит демократичної легітимності в алгоритмічному управлінні.

Р. Браунсворд у межах теорії «технологічного управління» наголошує, що сучасні держави дедалі частіше замінюють право технологічним контролем, що має глибокі наслідки для суверенітету та прав людини [6].

Український науковий дискурс нео-техносудверенітету формується в умовах постійних безпекових викликів, що зумовлює його прикладний та міждисциплінарний характер. Одним із ключових дослідників є Д. Дубов, який аналізує цифровий суверенітет у контексті інформаційної безпеки та державної політики [7]. Автор підкреслює, що для України цифровий суверенітет є не абстрактною теорією, а практичною умовою виживання держави.

Інформаційний суверенітет у працях українських науковців часто розглядається як складова національної безпеки, що відрізняє український підхід від західного, де акцент робиться на економічних і регуляторних аспектах цифрової автономії.

Значний внесок у розвиток теоретичних засад техносудверенітету зробили українські правознавці. О. Солодка аналізує його крізь призму конституційного права та прав людини, наголошуючи на необхідності пропорційності цифрових обмежень [8]. У її роботах техносудверенітет постає як правова

конструкція, що має бути врівноважена демократичними гарантіями. Милосердна І.М. і Краснопольська Т.М. досліджують трансформацію суверенітету в умовах цифровізації публічної влади, звертаючи увагу на зростання ролі алгоритмів у нормотворчих і управлінських процесах [9]. Цей підхід зближує український правовий дискурс із західними теоріями алгоритмічної влади, але водночас зберігає фокус на державному суверенітеті.

Особливістю української науки є тісний зв'язок теорії техносуперенітету з дослідженнями війни та гібридних загроз. А. Шульга аналізує цифровий суверенітет як ключовий елемент кібербезпеки та геополітичної стійкості держави [10]. У їхніх роботах кіберпростір розглядається як повноцінний вимір суверенної влади.

Ю. Калюжна, порівнюючи стратегії ЄС та України, доводить, що технологічна автономія є критичною умовою політичної незалежності в умовах війни [11]. Таким чином, український підхід інтегрує техносуперенітет у ширший безпековий дискурс.

Українські дослідження дедалі частіше розглядають саму Україну як емпіричний кейс трансформації суверенітету в цифрову епоху. Війна стимулює прискорене впровадження цифрових рішень, що дозволяє аналізувати техносуперенітет не лише теоретично, а й практично. У цьому сенсі українська наука робить внесок у глобальну теорію, пропонуючи досвід держави, що формує техносуперенітет в умовах екзистенційної загрози.

Метою статті є теоретичне осмислення нео-техносуперенітету як ключового тренду сучасної системи міжнародних відносин, а також виявлення його ролі як точки перетину між цифровим авторитаризмом і цифровою демократією на основі порівняльного аналізу зарубіжних теоретичних підходів і українського досвіду, сформованого в умовах війни та гібридних загроз.

Виклад основного матеріалу. Ключовою рисою нео-техносуперенітету є переосмислення big data як стратегічного ресурсу, дані дедалі частіше розглядаються як основа економічної конкурентоспроможності, національної безпеки та політичної стабільності. Саме тому держави прагнуть встановити контроль над потоками даних, локалізувати зберігання інформації або визначати правила доступу до неї. Шошанна Зубофф [12] доводить, що концентрація даних у руках приватних акторів створює асиметрії влади, які можуть підривати демократичні інститути, тоді як відповідь держави у вигляді нео-техносуперенітету часто має амбівалентний характер і балансує на межі між захистом громадян і посиленням контролю.

Іншим важливим виміром є технологічна автономія, в якій концепт нео-техносуперенітету передбачає здатність держави розробляти або принаймні контролювати ключові технології, від телекомунікаційних мереж і хмарних сервісів до систем штучного інтелекту та кібербезпеки. У цьому контексті дедалі частіше говорять про «цифровий суверенітет» як політичний проєкт, спрямований на зменшення залежності від глобальних технологічних гігантів і зовнішніх юрисдикцій [4]. Проте така автономія може реалізовуватися як у демократичному, так і в авторитарному ключі.

У сучасних дослідженнях міжнародних відносин, електронного урядування та трансформації політичних режимів, концепція нео-техносуперенітету дедалі частіше постає як ключовий аналітичний вузол, у якому перетинаються альтернативні траєкторії розвитку цифрових суспільств: від цифрової демократії до цифрового авторитаризму. Нео-техносуперенітет відображає прагнення держав зберегти або відновити контроль над власною цифровою інфраструктурою, даними, інформаційними потоками та алгоритмічними системами в умовах глобалізованого й платформізованого інформаційного простору.

У нормативному вимірі нео-техносуперенітет формується як відповідь на асиметрію влади між державами та транснаціональними технологічними корпораціями. Контроль над даними, платформами та алгоритмами дедалі частіше розглядається як складова національної безпеки, економічної стійкості та ідентичності. У демократичних політичних системах такий підхід може сприяти формуванню інклюзивних моделей електронного урядування, заснованих на захисті прав громадян, прозорості алгоритмів і підзвітності державних інституцій. У цьому сенсі нео-техносуперенітет виступає потенційним інструментом цифрової демократії, який дозволяє відновити публічний контроль над державним інформаційним простором та запобігти його повній або частковій приватній монополізації.

Водночас у державах із обмеженими демократичними традиціями або з кланово-олігархічною системою владних відносин, нео-техносуперенітет часто трансформується у передумову цифрового авторитаризму. Апелюючи до необхідності захисту суверенітету, держави розширюють практики обмеження прав людини: цифрового спостереження, цензури, алгоритмічного управління інформацією та превентивного контролю політичної поведінки громадян. У такому контексті технології стають не інструментом участі, а засобом управління і дисциплінування, що відповідає логіці авторитарних режимів в класичному їх розумінні, але із застосуванням ІКТ-інструментарію, за допомогою якого репресії замінюються тонкими механізмами маніпуляції, нагляду та превентивних дій.

З позиції синергетичного підходу, нео-техносуперенітет змінює функціональне призначення

інформаційно-комунікативної підсистеми суспільства. Якщо в умовах цифрової демократії вона орієнтована на забезпечення відкритого доступу до інформації, горизонтальні комунікації та плюралізму думок, то в авторитарному варіанті розвитку ця підсистема підпорядковується завданням контролю, селекції контенту та формування «дозволеного» інформаційного середовища. Таким чином, нео-техносуверенітет виступає точкою біфуркації, де вирішується, чи стане держава гарантом цифрових прав, чи їх головним обмежувачем.

У міжнародному вимірі нео-техносуверенітет сприяє фрагментації глобального інформаційного простору та формуванню конкуруючих моделей цифрового порядку. З одного боку, це відкриває можливості для розвитку альтернативних, більш етичних і правозахисних підходів до цифрового врядування, але з іншого, це створює умови для експорту цифрового авторитаризму, коли технології контролю та нормативні моделі обмеження свобод поширюються через міжнародні канали комунікації, технічну експансію та інфраструктурні проекти.

Особливе значення концепція набуває в умовах гібридних конфліктів та інформаційних воєн. Нео-техносуверенітет охоплює не лише технічний контроль, а й здатність держави захищати когнітивний простір суспільства від зовнішнього маніпулятивного впливу, дезінформації та психологічних операцій. У цьому сенсі він тісно пов'язаний із поняттями когнітивної безпеки, стратегічних комунікацій і цифрової дипломатії, що особливо актуально для держав, залучених до асиметричних конфліктів [13].

Разом із тим нео-техносуверенітет не є нормативно однозначною концепцією. У демократичних політичних системах він зазвичай інтерпретується як баланс між технологічною автономією, захистом прав людини та відкритістю глобальних комунікацій. Натомість в авторитарних режимах він часто трансформується в ідеологічне обґрунтування цифрового контролю, цензури та масового нагляду, що дозволяє легітимізувати обмеження свободи слова під прикриттям захисту національного суверенітету [14].

Повномасштабна війна російської федерації проти України стала безпрецедентним випробуванням для класичних уявлень про суверенітет та державну владу. В умовах постійних військових, кібернетичних, інформаційних, економічних та іміджевих атак Україна вимушено трансформує моделі управління, безпеки та комунікації, що фактично перетворює її на емпіричну лабораторію нео-техносуверенітету. У цьому контексті війна виступає не лише руйнівним чинником, а й тригером радикальної трансформації суверенітету.

Як вже було зазначено, класичне вестфальське розуміння суверенітету ґрунтується на чітко окресленій території, монополії на легітимне насильство та автономії політичного ухвалення рішень, проте в умовах гібридної війни ці параметри виявляються недостатніми. Український досвід демонструє, що контроль над територією не гарантує контролю над інформаційним простором, а військова сила не забезпечує захист від алгоритмічних, кібернетичних і платформних загроз.

У цьому сенсі війна актуалізує нео-техносуверенітет як форму функціональної влади, що реалізується через здатність держави зберігати керованість цифрових систем, забезпечувати безперервність передачі даних та комунікацій, інтегрувати приватних технологічних акторів у систему національної безпеки та швидко адаптувати правові та інституційні режими до нових технологічних викликів.

Україна вимушено реалізує ці функції в режимі реального часу, без «лабораторних» умов стабільності, що робить її досвід унікальним для теорії та практики побудови нео-техносуверенітету.

Однією з ключових характеристик українського нео-техносуверенітету стала стійкість цифрової держави, де попри масовані кібератаки на державні реєстри, телекомунікаційні системи та критичну інфраструктуру, Україна змогла зберегти функціонування основних цифрових сервісів, зокрема систем електронного врядування, публічних реєстрів та значно розширити ряд цифрових платформ, зробивши тим самим цифровий прорив як на рівні держави так і на рівні громадян, частина з яких, вимушено змінивши місце проживання, не втратила зв'язок з основними державними послугами.

Перенесення державних даних у хмарні середовища за підтримки міжнародних партнерів створило прецедент, в якому державна влада більше не прив'язана жорстко до території, такий підхід став вимушеним компромісом між безпекою та автономією, але водночас продемонстрував, що в умовах війни техносуверенітет не означає повної технологічної самодостатності, а радше здатність інтегрувати глобальні ресурси без втрати політичного контролю.

Кіберпростір у війні проти України перетворився на повноцінний театр бойових дій: кібератаки, операції з дестабілізації критичної інфраструктури, втручання в інформаційні системи та атаки на цифрову ідентичність громадян стали системним елементом агресії.

У відповідь Україна формує нову модель кіберсуверенітету, що стає джерелом стійкості та відповідає логіці постнекласичної державності шляхом поєднання державних інституцій з приватними ІТ-компаніями, волонтерськими кіберспільнотами та міжнародними партнерами, така мережева

модель управління безпекою підриває класичну ієрархію суверенної влади, але водночас підвищує адаптивність системи.

Особливе місце в українському досвіді займає боротьба за інформаційний суверенітет. Російська агресія супроводжується системними кампаніями дезінформації, маніпуляції алгоритмами соціальних мереж і використанням цифрових платформ як інструментів впливу [11].

Україна реагує на ці виклики шляхом управління алгоритмічними екосистемами (співпраці з платформами щодо модерації контенту) у яких держава є лише одним із акторів та демонструє, що інформаційний суверенітет у XXI столітті є не питанням цензури, а питанням домовленостей між державою та власниками цифрових платформ (інформаційних ТНК).

Війна створює перманентний стан надзвичайної ситуації, що суттєво впливає на правове регулювання взаємовідносин держава-громадянин у питанні цифрових обмежень, запроваджених із міркувань безпеки, і тут постає фундаментальне питання нео-техносуверенітету: при повоєнній відбудові куди поверне країна на перехресті між цифровим авторитаризмом і цифровою демократією.

Український кейс дозволяє емпірично дослідити, як війна легітимізує розширення технологічної влади держави та які механізми можуть стримувати її надмірну концентрацію.

Україна не лише адаптується до глобальних трендів техносуверенітету, а й стає активним тренд-сеттером цих змін, підтвердивши, що технології є ключовим ресурсом влади та показавши, що війна є каталізатором інституційної еволюції держави. У цьому сенсі Україна виступає не периферійним, а епістемічно центральним кейсом для теорії нео-техносуверенітету. Її досвід дозволяє переосмислити співвідношення між державою, технологіями та глобальними акторами в умовах екзистенційної загрози.

Висновки. У підсумку, нео-техносуверенітет слід розглядати не як альтернативу класичному суверенітету, а як його постнекласичну форму, що відображає структурні зміни влади в цифрову епоху, як перехрестя стратегічних виборів у розвитку цифрових політичних режимів, де його демократичний або авторитарний потенціал визначається якістю інституцій, рівнем громадянської участі, прозорістю цифрового регулювання та здатністю суспільства здійснювати контроль над владою. Саме в цій точці перетину вирішується, чи цифрові технології стануть інструментом розширення демократії, чи механізмом її поступової ерозії.

Нео-техносуверенітет це не просто нова форма державної політики, а глибока трансформація сутності влади у XXI столітті, що поєднує технологічні, політичні, економічні та етичні виміри, породжуючи нові виклики для традиційних моделей суверенітету, міжнародного права, міжнародних відносин та міжнародних комунікацій й демократичних інституцій.

Ця трансформація підкреслює, що влада все більше визначається не лише контролем над фізичною територією, а й контролем над цифровими потоками, даними та технологічними стандартами. У майбутньому успішні держави та інші актори, як державні, так і приватні, повинні будуть поєднувати технологічну автономію зі здатністю ефективно управляти ризиками, що супроводжують цифрову епоху.

Література

1. Held, D. (1995). *Democracy and the global order: From the modern state to cosmopolitan governance*. Stanford University Press.
2. Sassen, S. (1996). *Losing control? Sovereignty in an age of globalization*. Columbia University Press.
3. Castells, M. (2009). *Communication power*. Oxford University Press.
4. Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1–18. <https://doi.org/10.14763/2020.4.1532> (дата звернення: 23.01.2026)
5. Scharpf, F. W. (2018). Globalization and the erosion of national sovereignty. *European Review*, 26(1), 1–17. <https://doi.org/10.1017/S1062798717000468> (дата звернення: 23.01.2026)
6. Brownsword, R. (2019). *Law, technology and society: Re-imagining the regulatory environment*. Routledge.
7. Дубов Д.В. (2016) Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети*, 4(41), 9–24
8. Солодка О. (2020) Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. № 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) (дата звернення: 23.01.2026)
9. Милосердна І.М., Краснопольська Т.М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики*. 2022. Вип. 70. С. 106–113. <https://doi.org/10.32782/app.v70.2022.17> (дата звернення: 23.01.2026)

10. Шульга, А. М. Цифровий суверенітет як вид і проблема реального суверенітету держави / Шульга Анатолій Матвійович // Безпека у кіберсфері : зб. матеріалів Міжнар. наук.-практ. конф. (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ, Нац. акад. прав. наук України, Орг. з безпеки та співробітництва в Європі. – Кам'янець-Подільський: ХНУВС, 2025. – С. 243-244.

11. Калюжна Ю. (2025) Цифровий суверенітет як фактор національної безпеки ЄС та України. Національні інтереси України № 6(11), 1094-1124, [https://doi.org/10.52058/3041-1793-2025-6\(11\)-1094-1124](https://doi.org/10.52058/3041-1793-2025-6(11)-1094-1124) (дата звернення: 23.01.2026)

12. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

13. Santos Okholm, C., Ebrahimi Fard, A., & ten Thij, M. (2024). Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among the fringe communities of Western Europe. *Internet Policy Review*, 13(3). <https://doi.org/10.14763/2024.3.1788> (дата звернення: 23.01.2026)

14. Freedom House. (2023). Freedom on the Net 2023: The repressive power of artificial intelligence.

References

1. Held, D. (1995). *Democracy and the global order: From the modern state to cosmopolitan governance*. Stanford University Press.

2. Sassen, S. (1996). *Losing control? Sovereignty in an age of globalization*. Columbia University Press.

3. Castells, M. (2009). *Communication power*. Oxford University Press.

4. Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1–18. <https://doi.org/10.14763/2020.4.1532> (accessed January 23, 2026).

5. Scharpf, F. W. (2018). Globalization and the erosion of national sovereignty. *European Review*, 26(1), 1–17. <https://doi.org/10.1017/S1062798717000468> (accessed January 23, 2026).

6. Brownsword, R. (2019). *Law, technology and society: Re-imagining the regulatory environment*. Routledge.

7. Dubov, D. V. (2016). Stratehichni komunikatsii: problemy kontseptualizatsii ta praktychnoi realizatsii [Strategic communications: Problems of conceptualization and practical implementation]. *Stratehichni priorytety*, 4(41), 9–24. [in Ukrainian]

8. Solodka, O. (2020). Zabezpechennia informatsiinoho suverenitetu derzhavy: pravovyi dyskurs [Ensuring the information sovereignty of the state: A legal discourse]. *Informatsiia i pravo*, (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] (accessed January 23, 2026).

9. Myloserdna, I. M., & Krasnopolska, T. M. (2022). Protses tsyfrovizatsii v politytsi: mezhi piznannia ta osoblyvosti transformatsii [The process of digitalization in politics: Limits of cognition and features of transformation]. *Aktualni problemy polityky*, (70), 106–113. <https://doi.org/10.32782/app.v70.2022.17> [in Ukrainian] (accessed January 23, 2026).

10. Shulha, A. M. (2025). Tsyfrovyi suverenitet yak vyd i problema realnoho suverenitetu derzhavy [Digital sovereignty as a type and problem of real state sovereignty]. In *Bezpeka u kibersferi: Proceedings of the International Scientific and Practical Conference* (pp. 243–244). Kharkiv National University of Internal Affairs. [in Ukrainian]

11. Kaliuzhna, Yu. (2025). Tsyfrovyi suverenitet yak faktor natsionalnoi bezpeky YeS ta Ukrainy [Digital sovereignty as a factor of national security of the EU and Ukraine]. *Natsionalni interesy Ukrainy*, (6(11)), 1094–1124. [https://doi.org/10.52058/3041-1793-2025-6\(11\)-1094-1124](https://doi.org/10.52058/3041-1793-2025-6(11)-1094-1124) [in Ukrainian] (accessed January 23, 2026).

12. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

13. Santos Okholm, C., Ebrahimi Fard, A., & ten Thij, M. (2024). Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among the fringe communities of Western Europe. *Internet Policy Review*, 13(3). <https://doi.org/10.14763/2024.3.1788> (accessed January 23, 2026).

14. Freedom House. (2023). Freedom on the Net 2023: The repressive power of artificial intelligence.

Отримано: 24.01.2026

Прийнято до публікації: 06.04.2026

Опубліковано: 15.04.2026