

УДК 351.82: 342.34:004.056.5:342.228

JEL K10, H11, L86, O38

DOI: <https://doi.org/10.32782/2786-8273/2026-14-33>**Яременко О.І.**

кандидат наук з державного управління, доцент,
доцент кафедри публічного управління та менеджменту,
Вінницький державний педагогічний університет ім. М. Коцюбинського
ORCID: <https://orcid.org/0000-0002-3053-2257>

Oleksandr Yaremenko

Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University

Вітюк О.О.

кандидат історичних наук,
старший викладач кафедри публічного управління та менеджменту,
Вінницький державний педагогічний університет ім. М. Коцюбинського
ORCID: <https://orcid.org/0009-0007-1749-507X>

Oleksandr Vitiuk

Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University

ЦИФРОВИЙ СУВЕРЕНІТЕТ УКРАЇНИ: КОНСТИТУЦІЙНО-ПРАВОВІ ТА УПРАВЛІНСЬКІ АСПЕКТИ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

UKRAINE'S DIGITAL SOVEREIGNTY: CONSTITUTIONAL, LEGAL, AND ADMINISTRATIVE ASPECTS OF PROTECTING CRITICAL INFORMATION INFRASTRUCTURE

Анотація. У статті проаналізовано особливості цифрового суверенітету України як новітнього виміру державного суверенітету, а також окреслено ключові правові та управлінські виклики для функціонування критичної інформаційної інфраструктури в умовах повномасштабної збройної агресії з боку російської федерації. Доведено, що в умовах режиму воєнного стану цифровий суверенітет перетворюється з теоретичної категорії на гарантію функціональної спроможності держави. Виявлено проблеми міжвідомчої координації між суб'єктами забезпечення кібербезпеки. Обґрунтовано необхідність розширення концептуального тлумачення ст. 17 Конституції України шляхом включення кіберзахисту критичної інформаційної інфраструктури до системи найважливіших функцій держави. Результати дослідження можуть бути використані у нормотворчій діяльності вищих органів влади під час адаптації вітчизняного законодавства із цифровим правом ЄС.

Ключові слова: цифровий суверенітет, публічне управління, конституційне право, критична інформаційна інфраструктура, кібербезпека, державні реєстри, хмарні технології.

Abstract. Introduction. The russian federation's full-scale armed aggression against Ukraine marked a paradigm shift in modern interstate conflicts. Critical information infrastructure has become a target of cyberattacks. Under these circumstances, the functioning of government agencies and the preservation of the integrity of critical data have become essential prerequisites for effective governance. The concept of «digital sovereignty» serves as a tangible guarantee of national security, the functional resilience of public administration, and the preservation of the constitutional order. **Purpose.** The purpose of this article is to conduct a scholarly analysis of the nature of Ukraine's digital sovereignty as the latest transformational component of state sovereignty, and to identify systemic legal and administrative problems that hinder the functioning of critical information infrastructure during full-scale armed aggression. **Methods.** The study is based on the use of methodological tools from the fields of public administration theory and constitutional law. The research employs the systemic-structural method, comparative legal analysis, the functional approach, the formal-legal method, and the modeling method. **Results.** This article argues for the need to broaden the conceptual interpretation of Article 17 of the Constitution of Ukraine by including the cybersecurity of critical information infrastructure among the state's most important functions; it analyzes the governance risks associated with implementing a «Cloud First» policy under martial law; and it demonstrates the need to distinguish between different methods of processing government data. **Conclusion.** The study showed that the phenomenon of digital sovereignty is an integral component of Ukraine's state sovereignty. Ensuring cybersecurity and protecting critical information infrastructure is a constitutional obligation of the state to ensure information security. The existing model of public administration in this area has demonstrated its ability to adapt; however, it requires addressing issues related to interagency coordination, human resources, and improving the protection of critical information infrastructure at the local level.

Keywords: digital sovereignty, public administration, constitutional law, critical information infrastructure, cybersecurity, government registries, cloud technologies.

Постановка проблеми. Повномасштабна збройна агресія російської федерації проти України остаточно зафіксувала зміну парадигми сучасного протиборства: гібридна війна розгортається не лише у фізичному просторі, а й у кіберсфері. Об'єктами цілеспрямованих кібератак стають не тільки військові системи, а й критична інформаційна інфраструктура – державні реєстри, банківська система, енергетичні мережі, транспортні вузли та цифрові платформи надання публічних послуг.

У таких умовах безперебійне функціонування органів державної влади та захист даних громадян стають безпосередньою умовою збереження керованості державою. Це актуалізує концепт «цифрового суверенітету» не як абстрактної теоретичної категорії, а як реальної гарантії національної безпеки та конституційного порядку. Реалізація завдань цифрової трансформації публічного сектору вимагає чіткого визначення правових меж діджиталізації, щоб технічна ефективність електронного урядування не нівелювала конституційні права і свободи громадян.

Аналіз останніх досліджень і публікацій. Проблема державного суверенітету, а також національної та інформаційної безпеки посідає ключове місце у вітчизняних наукових дослідженнях. Концептуальні підходи до конституційно-правового осмислення державного суверенітету висвітлено у дослідженнях Барабаша Ю., Бориславської О., Венгера В., Козюбри М., Лисенка О., Мелешевича А. [6].

Конституційні наслідки та виклики цифрового суверенітету обґрунтовано у статті Новікова Є. [10]. Дослідник розглядає цифровий суверенітет у подвійному вимірі – як концептуальний виклик для сучасної політико-правової теорії та як чинник, що зумовлює реальні конституційні наслідки для окремих держав і наднаціональних союзів, зокрема Європейського Союзу. На думку автора, сучасна цифрова політика влади та міжнародних об'єднань тісно спирається на ідею цифрового суверенітету, яка все частіше звучить в офіційному політичному дискурсі. Ця робота вирізняється саме конституційно-правовим підходом до осмислення цифрового суверенітету, що відрізняє її від переважно політологічних чи кібербезпекових трактувань, поширених у сучасній науковій літературі.

У своїй публікації О. Никон [9] досліджує сутність «цифрового суверенітету», який спочатку формувався як здатність держави контролювати цифрову інфраструктуру у власних межах. Водночас авторка наголошує, що в контексті конституційного права пріоритетним є саме індивідуальний вимір такого суверенітету, оскільки він тісно пов'язаний із забезпеченням і захистом базових прав та свобод людини.

Розвитку цифрових комунікацій та свободи слова в епоху цифрових технологій присвячена стаття Кучин Т. та Костенко І. [8]. Автори наголошують, що стрімкий розвиток інтернету та цифрових комунікацій розширив не лише можливості для вільного обміну інформацією, а й загрози онлайн-переслідувань та цензури. Удосконалення й доступність цифрових інструментів дають змогу здійснювати жорсткіший контроль і заборони, що створює серйозні ризики для свободи слова та прав людини. Саме тому глибоке вивчення цієї проблематики є критично важливим для розробки ефективних

стратегій захисту прав і свобод громадян в епоху цифрових технологій.

Цифрові права людини поступово стають невіддільним елементом сучасного соціуму, де технології кардинально трансформують звичний спосіб життя та комунікації. Водночас Україна, подібно до інших держав, стикається з низкою викликів у цій сфері, викликаних динамічним поширенням інформаційно-комунікаційних технологій. Ознайомлення з цифровими правами, підкреслюють Белов Д., Переш І. та Пакорба І. [4], дає змогу громадянам розуміти, яким чином їхні персональні дані збираються, обробляються та зберігаються, а також допомагає ефективно захищати своє приватне життя.

Аналіз європейського досвіду формування нормативно-правової бази у сфері цифрового суверенітету створює надійне підґрунтя для вдосконалення вітчизняного законодавства та його подальшої імплементації. Ухвалення Регламенту GDPR у 2016 р. (Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [2] та європейського Акту про штучний інтелект у 2024 р. [3], помітно зміцнило нормативну основу індивідуального цифрового суверенітету на рівні вторинного законодавства ЄС. Регламент GDPR закріпив базові права суб'єктів персональних даних – зокрема право на доступ, виправлення, видалення чи заперечення проти обробки [2], Акт про штучний інтелект поглибив цю систему, заборонивши використання ШІ-систем із неприйнятним ступенем ризику та запровадивши жорсткі стандарти прозорості й контролю з боку людини [3].

Нормативно-правову базу дослідження склали Конституція України [7], Закони України «Про основні засади забезпечення кібербезпеки України» [13], «Про критичну інфраструктуру» [12], «Про захист персональних даних» [11], «Про публічні електронні реєстри» [14], «Про хмарні послуги» [16] та Рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» [15].

Метою статті є науковий аналіз сутності цифрового суверенітету України як новітнього трансформаційного компонента державного суверенітету, системно-правові та державно-адміністративні виклики, що впливають на функціонування критичної інформаційної інфраструктури під час повномасштабної збройної агресії, розробка юридично обґрунтованих пропозицій щодо оптимізації національного законодавства та механізмів державного управління з урахуванням стандартів європейської інтеграції.

Методи дослідження. Дослідження побудоване на використанні методологічного інструментарію теорії публічного управління та конституційного права. Застосовано системно-структурний метод (для побудови суб'єктно-об'єктної моделі критичної інформаційної інфраструктури), порівняльно-правовий аналіз (для порівняння вітчизняного законодавства із нормами Директиви ЄС NIS2 «Network and Information Security Directive 2» та положеннями GDPR), функціональний підхід (для аналізу повноважень спеціально уповноважених органів влади, відповідальних за сферу кібербезпеки), формально-юридичний метод (для тлу-

мачення норм ст. ст. 1, 17, 24, 32 та 64 Конституції України) та метод моделювання (для розробки трирівневої класифікації державних даних).

Виклад основного матеріалу дослідження. Розбудова цифрового середовища докорінно змінює традиційні державотворчі інститути, серед яких провідну позицію займає державний суверенітет. Ст. 1 Конституції України [7] проголошує Україну суверенною і незалежною державою, що традиційно передбачає верховенство влади всередині країни та її незалежність у зовнішніх зносинах.

З погляду конституційного права цифровий суверенітет доцільно сприймати не як окремих вид суверенітету, а як новітній вимір вияву верховенства та незалежності державної влади в цифровому просторі. Його сутність полягає в можливості держави самостійно, уникаючи стороннього несанкціонованого втручання, формувати цифрову та інформаційну політику, контролювати власні мережі й інфраструктуру, гарантувати безпеку державних баз даних, а також ефективно охороняти конституційні права громадян в онлайн-середовищі.

Базовим теоретико-правовим фундаментом для осмислення концепції цифрового суверенітету виступає ст. 17 Конституції України [7]. Вона проголошує охорону державного суверенітету, територіальної цілісності та гарантування інформаційної безпеки найголовнішими обов'язками держави і водночас справою всього українського народу. У контексті стрімкої цифрової еволюції зміст поняття «інформаційна безпека» суттєво розширюється, тісно переплітаючись із кібербезпекою та завданнями захисту критичної інформаційної інфраструктури.

Концептуальний аналіз дає змогу окреслити три основні конституційно-правові виміри цифрового суверенітету: просторово-територіальний аспект: законодавче закріплення цифрової інфраструктури в межах державного поля юрисдикції чи розробка ефективних конституційних гарантій контролю над нею під час використання екстериторіальних хмарних сервісів [16]; суб'єктно-владний вимір: гарантоване державі право приймати імперативні рішення стосовно функціонування власних інформаційних масивів, забезпечуючи незалежність від приватних технологічних монополій та іноземних юрисдикцій; правозахисний вимір: зобов'язання держави забезпечувати захист приватного життя (ст. 32 Конституції України [7], Закон України «Про захист персональних даних» [11]) та рівні можливості для громадян під час користування електронними послугами (ст. 24 Конституції України [7]) в контексті загальної цифровізації.

Отже, цифровий суверенітет виступає наріжним каменем захисту конституційного ладу. Відсутність здатності держави гарантувати безпеку своєї критичної інформаційної інфраструктури веде до ослаблення управлінських позицій у державі та становить пряму загрозу її національній безпеці.

Рівень дієвості цифрового суверенітету визначається якістю побудови державного управління у сфері забезпечення безпеки критичної інформаційної інфраструктури. На відміну від звичних об'єктів критичної інфраструктури, критична інформаційна інфраструктура відзначається стрімкою динамікою, глобальним характером зв'язків та підвищеною вразливістю до

прихованих кіберзагроз. Чинна модель публічного управління кіберзахистом критичної інформаційної інфраструктури в Україні ґрунтується на законах України «Про основні засади забезпечення кібербезпеки України» [13] і «Про критичну інфраструктуру» [12], а також на положеннях Стратегії кібербезпеки України [15]. Вони створюють розгалужену систему взаємодії суб'єктів та об'єктів, де головними важелями управлінського впливу постають: Рада національної безпеки і оборони України (шляхом діяльності Національного координаційного центру кібербезпеки), яка встановлює орієнтири державної політики та забезпечує узгодженість міжвідомчої взаємодії [15]; спеціально-уповноважені органи: Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ), яка виступає регулятором та адміністратором Держспецзв'язку, Служба безпеки України (проти кібертероризму та кібершпигунства), Національна поліція України (боротьба з кіберзлочинністю) та Міністерство оборони України разом із Збройними силами України (кібероборона) [13]; секторальний та об'єктовий рівні: Міністерства, інші центральні органи виконавчої влади (секторальні органи), а також безпосередньо оператори критичної інформаційної інфраструктури незалежно від форми власності [12].

Незважаючи на суттєві здобутки в процесі відбиття повномасштабної кіберагресії, чинна система публічного управління захистом критичної інформаційної інфраструктури, на нашу думку, стикається з низкою серйозних системних викликів, зокрема, це складнощі у міжвідомчій взаємодії та функціональний дубляж (існування кількох суб'єктів із паралельними повноваженнями щодо протидії кіберінцидентам подекуди викликає розсіювання відповідальності та затримки в оперативному прийнятті управлінських рішень; дефіцит фахівців у державній сфері (гостра конкуренція з приватним ринком праці за кіберекспертів створює постійний дисбаланс, подолання якого ускладнюється жорсткими рамками стандартної тарифної сітки та заробітних плат державних службовців; нерівномірність технічного оснащення операторів критичної інформаційної інфраструктури (об'єкти критичної інформаційної інфраструктури комунальної власності та органів місцевого самоврядування нерідко демонструють суттєво нижчий рівень захищеності порівняно з центральними державними відомствами чи банками, що перетворює їх на «слабку ланку» в загальній системі національної кібербезпеки). Досвід війни продемонстрував, що звичні бюрократичні механізми регулювання критичної інформаційної інфраструктури потребують підвищеної гнучкості. Публічне управління в цій сфері має еволюціонувати від пасивного нагляду за дотриманням формальних стандартів до проактивного управління ризиками в реальному часі, що охоплює постійний моніторинг та автоматизований обмін даними про загрози.

З початком повномасштабного вторгнення російської федерації критичним випробуванням для цифрового суверенітету України виявилася потреба зберегти фізичну та функціональну недоторканність державних даних. Ризики знищення серверів унаслідок обстрілів чи їх окупації зумовили необхідність екстреної, проте правомірно обґрунтованої релокації держреєстрів і критичної інфраструктури до міжна-

родних хмарних сховищ відповідно до Законів України «Про хмарні послуги» [16] та «Про публічні електронні реєстри» [14].

Перехід на хмарні рішення (Cloud First Policy) та транскордонна міграція державних масивів даних зумовили появу нових управлінсько-правових реалій, які характеризуються певним спектром суперечностей, зокрема, розташування національних реєстрів [14] на закордонних серверах комерційних компаній автоматично поширює на них правові режими країн-резидентів цих корпорацій, що в свою чергу створює серйозну правову колізію, за якої іноземні правоохоронні органи можуть витребувати українські державні дані поза межами офіційних процедур міжнародно-правового співробітництва, а також, транскордонне переміщення персональних даних [11] українських громадян потребує неухильного дотримання високих стандартів їх безпеки, як наслідок, це формує складне управлінське завдання – забезпечити повну відповідність передачі інформації до зарубіжних хмарних платформ вимогам регламенту GDPR, не допускаючи водночас порушень конституційного права громадян на захист приватного та сімейного життя. Також, слід зауважити, що більшість рішень про дозвіл на розташування державних баз даних за межами країни ухвалювалася як тимчасовий антикризовий захід в умовах воєнного стану, а чинна нормативна база вимагає формування чіткої стратегії в післявоєнний, яка б передбачала розмежування категорій інформації: одні масиви зможуть постійно зберігатися у хмарах, тоді як інші підлягатимуть обов'язковому поверненню на національну територію з міркувань державної безпеки.

Таким чином, застосування хмарних технологій вимагає пошуку оптимального конституційно-правового балансу між невіддільною потребою в безперервному наданні державних послуг та імперативом збереження суверенного права на абсолютний контроль над власними інформаційними ресурсами.

Для подолання наявних системних суперечностей і зміцнення моделі цифрового суверенітету України необхідна всебічна модернізація нормативно-правового поля та вдосконалення управлінських інструментів. З огляду на результати аналізу, визначено ключові напрями оптимізації, такі як:

1. Законодавче закріплення поняття «цифровий суверенітет» та класифікація даних (потребуватиме внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України» [13], з необхідністю чіткого визначення дефініції цифрового суверенітету та його складових). Також, законодавчо слід імплементувати трирівневу градацію державних даних: категорії інформації підвищеної важливості (оборона, державна безпека, вищі органи влади), розміщення яких дозволене виключно в межах національного простору України на захищених серверних потужностях; дані обмеженого доступу та реєстрові записи, які дозволено зберігати на гібридних хмарних платформах завдяки обов'язковому шифруванню згідно з національними протоколами за збереження контролю

над ключами дешифрування за ДССЗ31 [16]; відкриті публічні дані, які можуть без обмежень оброблятися у публічних хмарах.

2. Повноцінна інтеграція України до європейського цифрового простору вимагає імплементації норм Директиви ЄС щодо кібербезпеки (NIS2 Directive [1]), що передбачає розширення кола суб'єктів критичної інформаційної інфраструктури завдяки включенню провайдерів цифрових послуг, установлення персональної юридичної відповідальності керівників таких суб'єктів за нехтування правилами кібергігієни, а також запровадження обов'язку інформувати про кіберінциденти впродовж 24 годин.

3. Реформування публічного управління захистом критичної інформаційної інфраструктури має супроводжуватися розробкою чітких законодавчих запобіжників від надмірного втручання держави у приватне життя громадян під час проведення протиаварійних або контррозвідувальних заходів у кіберпросторі, гарантуючи судовий контроль та дотримання принципів пропорційності (Ст. 64 Конституції України) [7].

Висновки. У результаті проведеного дослідження визначено, що в умовах цифрової трансформації та повномасштабної збройної агресії феномен цифрового суверенітету є невід'ємною складовою державного суверенітету України, визначеного ст. 1 Конституції України. Він полягає у спроможності держави самостійно визначати цифрову політику, контролювати власну інформаційну інфраструктуру та забезпечувати конституційні гарантії прав громадян у кіберпросторі.

Визначено, що забезпечення кібербезпеки та захисту критичної інформаційної інфраструктури виступає безпосередньою реалізацією конституційного обов'язку держави щодо забезпечення інформаційної безпеки. Існуюча модель публічного управління захистом критичної інформаційної інфраструктури проявила високу адаптивність під час війни, однак зіштовхується із викликами міжвідомчої взаємодії, кадрового дефіциту та нерівномірності захисту об'єктів критичної інформаційної інфраструктури на місцевому рівні.

З'ясовано, що масовий перехід на використання закордонних хмарних інфраструктур дозволив зберегти державні реєстри від фізичного знищення, проте створив нові правові суперечності. Головними з них є загроза виникнення юрисдикційних конфліктів із законодавством країн-резидентів хмарних провайдерів, потенційне втручання у право на приватність та відсутність законодавчо визначеної післявоєнної стратегії повернення даних.

Пропонуємо розробити та затвердити Стратегію збереження та управління державними електронними інформаційними ресурсами у післявоєнний період, розмежувавши режими використання національних та закордонних дата-центрів, а також, удосконалити єдині технічні регламенти та стандарти шифрування для державних даних, які зберігаються у хмарних сховищах, із обов'язковим утриманням контролю над ключами шифрування за уповноваженими державними органами України.

Бібліографічний список:

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. L 119, 4.5.2016. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
4. Белов Д.М., Переш І.Є., Покорба І. Цифрові права людини: доктринальні засади. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 110–115. DOI: <https://doi.org/10.24144/2788-6018.2024.02.17>.
5. Колісник В.П. Вплив взаємодії вищих органів державної влади на забезпечення державного суверенітету України. *Організаційні та правові проблеми забезпечення державного суверенітету* : матеріали міжнар. наук.-практ. конф., м. Харків, 27 березня 2009 р. С. 19–21.
6. Конституційне право: підручник / Ю.Г. Барабаш та ін. ; за заг. ред. М.І. Козюбри. Київ : ВАІТЕ, 2021. 528 с.
7. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
8. Кучин Т.Р., Костенко І.В. Свобода слова в епоху цифрових технологій: захист від цензури та онлайн-переслідувань. *Науковий вісник Ужгородського Національного Університету. Серія «Право»* 2024. Вип. 83, ч. 1. С. 130–135. DOI: <https://doi.org/10.24144/2307-3322.2024.83.1.18>.
9. Никон О. З. Цифровий суверенітет особи як конституційна цінність. *Науковий вісник Ужгородського Національного Університету. Серія «Право»*. 2026. Вип. 95. С. 479–488. DOI: <https://doi.org/10.24144/2307-3322.2026.95>.
10. Новіков Є. Цифровий суверенітет: концептуальні виклики та конституційні наслідки. *Конституційно-правові академічні студії*. 2024. № 1. С. 61–69. DOI: <https://doi.org/10.24144/2663-5399.2024.1.08>.
11. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297–VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.
12. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882–IX. Відомості Верховної Ради України. 2022. № 11. Ст. 74.
13. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163–VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.
14. Про публічні електронні реєстри : Закон України від 18 листопада 2021 р. № 1907–IX. Відомості Верховної Ради України. 2022. № 13. Ст. 88.
15. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. Офіційний вісник Президента України. 2021. № 20. Ст. 855.
16. Про хмарні послуги : Закон України від 17 лютого 2022 р. № 2075–IX. Відомості Верховної Ради України. 2022. № 18. Ст. 128.

References:

1. Dyrektyva (EU) 2022/2555 Yevropeiskoho Parlamentu ta Rady vid 14 hrudnia 2022 roku pro zakhody shchodo vysokoho spilnoho ravnia kiberbezpeky v Soiuzi [Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union]. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.
2. Rehlament (EU) 2016/679 Yevropeiskoho Parlamentu ta Rady vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zviazku z obrobkoiu personalnykh danykh ta pro vilnyi rukh takykh danykh, ta skasuvannia Dyrektyvy 95/46/EC (Zahalnyi rehlament zakhystu danykh) [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)]. *Ofitsiyni visnyk Yevropeiskoho Soiuzu*. L 119, 4.5.2016. P. 1–88. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
3. Rehlament (IeS) № 2024/1689 Yevropeiskoho Parlamentu ta Rady vid 13 chervnia 2024 roku, yakym vstanovliuiutsia harmonizovani pravyla shchodo shtuchnoho intelektu [Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)]. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
4. Bielov D.M., Peresh I.Ie., Pokorba I. (2024). Tsyfrovi prava liudyny: doktrynalni zasady [Digital Human Rights]. *Analychno-porivnialne pravoznavstvo*, vol. 2. pp. 110–115. DOI: <https://doi.org/10.24144/2788-6018.2024.02.17>. (in Ukrainian).
5. Kolisnyk V.P. (2009). Vplyv vzaiemodii vyshchych orhaniv derzhavnoi vlady na zabezpechennia derzhavnoho suverenitetu Ukrainy [The Impact of Interaction Among the Higher State Authorities on Ensuring Ukraine's State Sovereignty]. *Orhanizatsiini ta pravovi problemy zabezpechennia derzhavnoho suverenitetu* : materialy mizhnar. nauk.-prakt. konf., (Kharkiv, March 27, 2009. pp. 19–21. (in Ukrainian).
6. Konstytutsiine pravo: pidruchnyk (2021) [Constitutional Law: Textbook]. Yu.H. Barabash ta in. ; za zah. red. M.I. Koziubry. Kyiv : VAITE, 528 p. (in Ukrainian).
7. Konstytutsiia Ukrainy : Zakon Ukrainy vid 28 chervnia 1996 r. № 254k/96-VR [The Constitution of Ukraine] / Verkhovna Rada Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy*. 1996. № 30. St. 141. (in Ukrainian).
8. Kuchyn T.R., Kostenko I.V. (2024). Svoboda slova v epokhu tsyfrovyykh tekhnolohii: zakhyst vid tsenzury ta onlain-peresliduvan [Freedom of Speech in the Digital Age: Protection Against Censorship and Online Harassment]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia "Pravo"*, vol. 83 (1). pp. 130–135. DOI: <https://doi.org/10.24144/2307-3322.2024.83.1.18>. (in Ukrainian).
9. Nykon O. Z. (2026). Tsyfrovyi suverenitet osoby yak konstytutsiina tsinnist [Digital Sovereignty of the Individual as a Constitutional Value]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia "Pravo"*, vol. 95. pp. 479–488. DOI: <https://doi.org/10.24144/2307-3322.2026.95>. (in Ukrainian).

10. Novikov Ye. (2024). Tsyfrovyi suverenitet: kontseptualni vyklyky ta konstytutsiini naslidky [Digital Sovereignty: Conceptual Challenges and Constitutional Implications]. Konstytutsiino-pravovi akademichni studii. № 1. pp. 61–69. DOI: <https://doi.org/10.24144/2663-5399.2024.1.08>. (in Ukrainian).
11. Pro zakhyst personalnykh danykh : Zakon Ukrainy vid 1 chervnia 2010 r. № 2297–VI [On the Protection of Personal Data]. Vidomosti Verkhovnoi Rady Ukrainy. 2010. № 34. St. 481. (in Ukrainian).
12. Pro krytychnu infrastrukturu : Zakon Ukrainy vid 16 lystopada 2021 r. № 1882–IX [On Critical Infrastructure]. Vidomosti Verkhovnoi Rady Ukrainy. 2022. № 11. St. 74. (in Ukrainian).
13. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163–VIII On the Basic Principles of Ensuring Cybersecurity in Ukraine. Vidomosti Verkhovnoi Rady Ukrainy. 2017. № 45. St. 403. (in Ukrainian).
14. Pro publichni elektronni reiestry : Zakon Ukrainy vid 18 lystopada 2021 r. № 1907–IX [On Public Electronic Registers]. Vidomosti Verkhovnoi Rady Ukrainy. 2022. № 13. St. 88. (in Ukrainian).
15. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku “Pro Stratehiu kiberbezpeky Ukrainy” : Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 r. № 447/2021 [On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, “On the Cybersecurity Strategy of Ukraine”]. Ofitsiinyi visnyk Prezydenta Ukrainy. 2021. № 20. St. 855. (in Ukrainian).
16. Pro khmarni posluhy : Zakon Ukrainy vid 17 liutoho 2022 r. № 2075–IX [On Cloud Services]. Vidomosti Verkhovnoi Rady Ukrainy. 2022. № 18. St. 128. (in Ukrainian).

Дата надходження статті: 24.07.2026

Дата прийняття статті до публікації: 17.09.2026

Дата публікації статті: 30.09.2026