

*Сергій Анатолійович Люлько,  
аспірант відділу теорії держави і права  
Інституту держави і права  
імені В. М. Корецького НАН України  
ORCID: 0009-0004-5704-3738*

## ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ: СТРУКТУРА І ФУНКЦІЇ

**Постановка проблеми.** Глобалізація інформаційних потоків і цифрова трансформація суспільства створюють принципово нові виклики для державного суверенітету. Якщо традиційне розуміння суверенітету базувалося на територіальному принципі та фізичних кордонах держави, то сучасний цифровий простір характеризується екстериторіальністю, транснаціональністю інформаційних потоків та зростанням впливу недержавних акторів – глобальних технологічних платформ. Інформаційний суверенітет як здатність держави контролювати національний інформаційний простір та забезпечувати інформаційну безпеку набуває критичного значення для захисту національних інтересів, демократичних інститутів та прав громадян. Для України, яка протистоїть масштабній інформаційній агресії російської федерації, питання структурної організації та функціонального призначення інформаційного суверенітету є особливо актуальними та потребують глибокого теоретико-правового осмислення.

Водночас сучасна юридична наука ще не виробила усталеного розуміння структури та функцій інформаційного суверенітету як правової категорії. Наявні дослідження, як правило, зосереджуються або на окремих аспектах правового регулювання інформаційного простору, або на загальнотеоретичних проблемах державного суверенітету в умовах глобалізації, не забезпечуючи їх системного поєднання. Відсутність цілісного теоретико-правового підходу до структурних компонентів інформаційного суверенітету та його функцій суттєво ускладнює як наукову розробку відповідної проблематики, так і практичну діяльність державних органів щодо забезпечення інформаційної безпеки. Це зумовлює необхідність комплексного дослідження інформаційного суверенітету із застосуванням інструментарію загальної теорії держави і права.

**Аналіз останніх досліджень і публікацій.** Проблематику інформаційного суверенітету держави активно досліджують сучасні українські та зарубіжні науковці. Серед українських дослідників проблематика державного суверенітету та його інформаційної складової досліджується у працях С. Бобровник, С. Гусарева, О. Данильяна, Н. Оніщенко, О. Петришина, Н. Пархоменко, О. Радутного, В. Тернавської, Ю. Шемшученка та інших вчених, які аналізують проблеми розвитку сучасного державного суверенітету та правової системи, а також філософсько-правові виміри інформаційного суспільства. Серед зарубіжних дослідників цієї проблематики варто відзначити праці Е. Лейтера, Ш. Зубофф, Е. Селесте та ін. Водночас, незважаючи на значний науковий доробок цих та інших вчених стосовно цієї проблематики, системний аналіз структурних елементів інформаційного суверенітету та його функцій все ще залишається недостатньо дослідженим, зокрема в контексті теорії держави і права, що зумовлює необхідність подальших наукових розвідок у цьому напрямі.

**Мета статті** полягає у визначенні структурних компонентів інформаційного суверенітету держави та характеристиці його основних функцій.

**Основні результати дослідження.** Розуміння природи інформаційного суверенітету держави в сучасній юридичній доктрині характеризується множинністю підходів та відсутністю усталеної дефініції. В. Тернавська визначає інформаційний суверенітет як здатність держави контролювати інформаційні процеси на власній території та забезпечувати інформаційну безпеку, що відображає прагнення поширити традиційні суверенні повноваження на цифровий простір [1, с. 83]. О. Солодка акцентує увагу на правовому вимірі цього феномену, розглядаючи інформаційний суверенітет як сукупність правових норм і механізмів, що забезпечують незалежність держави у формуванні інформаційної політики [2, с. 85]. Є. Новіков виокремлює поняття цифрового суверенітету як

можливості держави самостійно визначати правила функціонування цифрового простору в межах своєї юрисдикції [3, с. 62].

Зазначені дефініції, попри певні відмінності у формулюваннях, концентруються навколо спільного розуміння інформаційного суверенітету як правової категорії, що відображає владні повноваження держави щодо регулювання інформаційного простору. Водночас варто підкреслити, що інформаційний суверенітет не є окремим видом суверенітету, а являє собою специфічний прояв єдиного державного суверенітету в інформаційній сфері. Це узгоджується із загальнотеоретичною позицією, сформульованою, з-поміж іншого, у підручнику «Теорія держави і права. Академічний курс», підготовленому за редакцією О. Зайчука і Н. Оніщенко, щодо цілісності та неподільності державного суверенітету як фундаментальної характеристики держави [4]. О. Петришин наголошує, що суверенітет держави реалізується через різноманітні сфери суспільного життя, зберігаючи при цьому свою єдність [5, с. 80]. Тож інформаційний суверенітет доцільно розглядати як функціональний вимір державного суверенітету, що стосується здатності держави здійснювати владу в національному сегменті інформаційного простору.

Важливість правильного визначення структури інформаційного суверенітету зумовлена необхідністю системного захисту інформаційної, а отже, національної безпеки держави. С. Бобровник підкреслює, що ефективність правового регулювання залежить від чіткого розуміння структурних елементів регульованих явищ [6]. Аналіз наукових підходів та практики забезпечення інформаційної безпеки дає змогу виокремити п'ять взаємопов'язаних компонентів структури інформаційного суверенітету.

Першим таким елементом є територіально-юрисдикційний компонент інформаційного суверенітету, який стосується поширення державної влади на інформаційні процеси, що відбуваються на території держави або стосуються її громадян. Зокрема, Е. Селесте обґрунтовує концепцію «цифрового конституціоналізму», що передбачає поширення конституційних принципів на онлайн-середовище та визнання цифрових прав як фундаментальних [7, с. 76]. Ця позиція заслуговує на підтримку, оскільки дає змогу забезпечити послідовність правового регулювання як у фізичному, так і в цифровому просторі. Водночас поширення юрисдикції держави на кіберпростір стикається з проблемою екстериторіальності цифрового середовища. Дж. Даскал, наприклад, досліджує феномен «нетериторіальності даних», коли інформація може одночасно перебувати у різних юрисдикціях [8, с. 333–334]. Це створює об'єктивні обмеження для реалізації територіального принципу суверенітету та потребує міжнародної координації у встановленні правил функціонування глобального інформаційного простору.

Ще одним компонентом інформаційного суверенітету держави є нормативно-правовий, який включає в себе систему законодавчого регулювання інформаційної сфери. Н. Пархоменко наголошує на ключовій ролі джерел права в забезпеченні ефективності правового регулювання [9]. Сучасна світова практика демонструє різні моделі правового забезпечення інформаційного суверенітету. Китайський підхід, втілений у Законі Китайської Народної Республіки про кібербезпеку 2017 року [10], базується на принципах жорсткої локалізації даних та пріоритету державної безпеки над індивідуальними правами. Європейський підхід, представлений насамперед Загальним регламентом про захист даних (GDPR) [11] та Актом про цифрові послуги, прагне збалансувати захист прав користувачів та обмеження домінування технологічних платформ [12, с. 3]. Американський підхід традиційно базується на секторальному регулюванні та принципах вільного Інтернету. Україна формує власну модель, закріплену у Конституції України від 28 червня 1996 року, Законі України «Про національну безпеку України» від 21 червня 2018 року, Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року та Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021. М. Шевчук аналізує систему національного законодавства про інформаційну безпеку, виявляючи як досягнення, так і прогалини у відповідному правовому регулюванні [13, с. 384]. Вважаємо, що оптимальна модель має поєднувати ефективний захист національних інтересів з дотриманням демократичних принципів та міжнародних стандартів прав людини.

Ще одним елементом інформаційного суверенітету держави є технологічний, який охоплює контроль над критичною інформаційною інфраструктурою, розвиток власних технологічних платформ і засобів кіберзахисту. С. Гусарев і О. Тихомиров підкреслюють, що матеріально-технічне

забезпечення є необхідною передумовою реалізації державних функцій [14, с. 52], у зв'язку із чим технологічна залежність від іноземних платформ і програмного забезпечення створює вразливості для національної безпеки та обмежує можливості здійснення суверенних повноважень у цифровому просторі. Без розвитку власних технологій кіберзахисту, шифрування, обробки даних тощо інформаційний суверенітет залишатиметься переважно формальним явищем, що є особливо актуальним для України в умовах протидії кіберагресії.

Наступним елементом інформаційного суверенітету держави слід визнати інформаційно-змістовий, який стосується контролю над інформаційним контентом, протидії дезінформації та забезпечення якості інформаційного середовища. У зазначеному контексті О. Радутний, наприклад, застерігає проти надмірного контролю над інформаційним простором, який може призвести до обмеження свободи слова та створення «ілюзії інформаційного суверенітету» [15, с. 3–32]. Підтримуємо цю позицію, оскільки надмірні обмеження суперечать демократичним цінностям. Саме тому важливим є необхідність забезпечення оптимального балансу між інформаційною безпекою та дотриманням демократичних принципів [1, с. 85], а також ефективного механізму правового регулювання інформаційного простору [2, с. 87], що має запобігати свавільному втручання держави.

Нарешті, міжнародно-правовий компонент інформаційного суверенітету відображає участь держави у формуванні міжнародних правил поведінки у кіберпросторі та захист національних інтересів на глобальному рівні. О. Дзьобань аналізує взаємозв'язок між розвитком інформаційних комунікацій та проблемою безпеки держави у глобалізованому суспільстві [16]. М. Шмітт систематизує принципи міжнародного права, застосовні до кіберпростору, включаючи суверенітет, невтручання, пропорційність [17, с. 75]. Проте застосування цих принципів залишається проблематичним через складність атрибуції кібератак і відсутність консенсусу щодо «порогу» порушення суверенітету.

Отже, наведені вище структурні компоненти інформаційного суверенітету держави формують цілісну систему, ефективність якої залежить від збалансованого розвитку всіх елементів. Правове регулювання без технологічного забезпечення залишається декларативним, технологічні можливості без правових рамок можуть призвести до зловживань, а контроль над контентом без міжнародної співпраці не може бути достатнім в умовах функціонування глобального інформаційного простору. У зв'язку із цим, лише системний підхід до розвитку всіх компонентів забезпечує реальний, а не ілюзорний інформаційний суверенітет держави.

Функціональне призначення інформаційного суверенітету реалізується через систему взаємопов'язаних функцій. О. Петришин визначає функції держави як основні напрями її діяльності, що виражають сутність та призначення держави [5, с. 89]. Виходячи з цього методологічного підходу, можемо виокремити п'ять основних функцій інформаційного суверенітету, а саме: захисна, регуляторна, розвиваюча, координаційна та міжнародно-представницька.

Так, захисна функція інформаційного суверенітету держави спрямована на охорону національного інформаційного простору від зовнішніх загроз – кібератак, деструктивних інформаційних впливів, іноземного втручання. У зазначеному контексті О. Гічко досліджує інформаційний суверенітет як передумову міжнародної співпраці України, особливо в умовах збройної агресії [18, с. 275], а С. Куцепал аналізує виклики для інформаційного суверенітету України у воєнний час [19, с. 81–82]. Вважаємо, що захисна функція є базовою, оскільки без захисту інформаційного простору в умовах сучасного технологічного розвитку неможливо забезпечити належну реалізацію інших функцій держави. При цьому слід враховувати, що захист національного інформаційного простору держави повинен здійснюватися на засадах верховенства права як основоположного принципу розвитку демократичних правових систем, у тому числі з урахуванням принципу пропорційності у праві і не повинен перетворюватися на тотальний контроль з боку держави, що суперечило б демократичним цінностям.

Регуляторна функція інформаційного суверенітету держави проявляється у встановленні законодавчих правил функціонування національного інформаційного простору, ліцензуванні діяльності у сфері медіа та поширення інформації, а також стандартизації відповідних технологій. Н. Оніщенко підкреслює, що ефективність правового регулювання залежить від рівня адекватності правових норм функціонуючим у суспільстві відносинам [4]. Регуляторна функція інформаційного суверенітету має забезпечувати баланс між державним контролем і свободою інформації, між

безпекою та інноваціями. При цьому надмірне правове регулювання може суттєво загальмувати розвиток цифрової економіки, а недостатнє – призвести до хаосу та загроз національній безпеці загалом.

Розвиваюча функція інформаційного суверенітету спрямована на створення умов для забезпечення ефективного розвитку національних інформаційно-комунікаційних технологій, цифрової економіки, підвищення інформаційної грамотності населення тощо. Так, С. Гусарев наголошує на важливості забезпечення умов для прогресивного розвитку суспільства [14, с. 52]. Саме тому без реалізації розвиваючої функції інформаційний суверенітет залишатиметься переважно декларативним, оскільки технологічна залежність або відсталість унеможлиблює реальну незалежність сучасних держав, які повинні інвестувати у цифрову інфраструктуру, підтримувати вітчизняні технологічні компанії, а також розвивати освіту у сфері інформаційних технологій.

Координаційна функція інформаційного суверенітету держави забезпечує передусім узгодження дій органів публічної влади та відповідних інститутів громадянського суспільства в національному сегменті інформаційного простору. С. Бобровник підкреслює важливість координації для ефективності правової системи [6], що є особливо важливим також для сучасної інформаційної сфери, яка потребує забезпечення ефективної взаємодії різноманітних інституцій: органів національної безпеки, правоохоронних органів, регуляторів телекомунікацій, органів захисту персональних даних, технологічних компаній тощо. Відсутність же належної координації визначених суб'єктів у інформаційному просторі призводить до дублювання відповідних функцій і зниження ефективності діяльності учасників інформаційних правовідносин.

Міжнародно-представницька функція інформаційного суверенітету держави реалізується через її участь у формуванні міжнародних норм управління Інтернетом, укладанні угод про кібербезпеку, роботі міжнародних організацій тощо. У цьому контексті О. Дзьобань, наприклад, аналізує роль інформаційних комунікацій у системі міжнародних відносин та проблеми забезпечення безпеки держави [16]. Зокрема, Україна бере участь у роботі групи урядових експертів ООН з питань інформаційної безпеки, співпрацює з НАТО у сфері кіберзахисту, імплементує європейські стандарти. Ефективна реалізація цієї функції дає змогу захищати національні інтереси на міжнародному рівні та впливати на формування відповідних правил.

Отже, навіть побіжний аналіз змісту зазначених функцій інформаційного суверенітету держави надає можливість зробити висновок, що всі вони є взаємопов'язаними між собою та взаємодоповнюють одна одну. Адже захист без розвитку веде до технологічного відставання; розвиток без регулювання може створити хаос у відповідних відносинах; регулювання без забезпечення належної координації не може бути ефективним; міжнародна співпраця без захисту національних інтересів призводить до фактичної втрати суверенітету. Саме тому лише збалансована реалізація всіх функцій забезпечує ефективність інформаційного суверенітету держави.

Водночас слід звернути увагу також на те, що наведені аспекти структури та функцій інформаційного суверенітету надають можливість виявити окремі проблеми та виклики його сучасного розвитку. По-перше, існує внутрішня напруженість між прагненням держави до контролю над інформаційним простором і необхідністю забезпечення свободи інформації як фундаментального права людини. При цьому надмірний контроль в інформаційній сфері може призвести до авторитаризму, а недостатній – залишити суспільство беззахисним. По-друге, глобальний характер інформаційних потоків обмежує можливості національного регулювання через об'єктивну екстериторіальність кіберпростору, що значно ускладнює здійснення належного владного впливу сучасних держав навіть на внутрішній інформаційний простір. По-третє, швидкість технологічних змін перевищує можливості правової системи адекватно реагувати на їх розвиток, створюючи відповідні регуляторні прогалини, які практично неможливо своєчасно усувати. По-четверте, розбудова виваженої моделі інформаційного суверенітету в сучасній Україні суттєво ускладнюється ще й необхідністю забезпечення одночасної протидії зовнішній інформаційній агресії з боку рф та збереження відкритості національного інформаційного простору, а також свободи слова, що потребує застосування особливих підходів до забезпечення національного інформаційного суверенітету.

**Висновки.** З урахуванням викладеного можна зробити такі висновки:

1. Інформаційний суверенітет держави являє собою багатоаспектне явище, що проявляється на структурному та функціональному рівнях як специфічний вимір єдиного державного суверенітету

в інформаційній сфері. Множинність підходів до визначення інформаційного суверенітету в сучасній юридичній доктрині свідчить про складність цього феномену та необхідність подальшого теоретико-правового осмислення його природи, меж та способів реалізації в умовах функціонування глобального цифрового простору.

2. Структура інформаційного суверенітету держави містить п'ять взаємопов'язаних компонентів: територіально-юрисдикційний, нормативно-правовий, технологічний, інформаційно-змістовий та міжнародно-правовий, які в сукупності формують цілісну систему забезпечення здатності держави контролювати національний інформаційний простір. Ефективність інформаційного суверенітету залежить від збалансованого розвитку всіх структурних компонентів, оскільки слабкість будь-якого з них підриває загальну спроможність держави захищати свої інтереси в інформаційній, зокрема цифровій, сфері, а також забезпечувати національну безпеку в умовах зростаючих інформаційних загроз.

3. Функціональне призначення інформаційного суверенітету реалізується через захисну, регуляторну, розвиваючу, координаційну та міжнародно-представницьку функції, гармонійна реалізація яких є необхідною умовою ефективного забезпечення інформаційної безпеки держави. У контексті сучасних викликів, зокрема інформаційної агресії проти України, особливого значення набуває збалансована реалізація захисної функції інформаційного суверенітету при збереженні демократичних цінностей, розвиваючої функції для подолання технологічної залежності та міжнародно-представницької функції для формування сприятливого міжнародно-правового регулювання та забезпечення ефективної співпраці України з відповідними міжнародними інституціями.

#### Список використаних джерел

1. Тернавська В. М. Концепція державного суверенітету в аспекті глобального інформаційного простору. *Інформація і право*. 2021. № 4 (39). С. 80–89. DOI: [https://doi.org/10.37750/2616-6798.2021.4\(39\).248794](https://doi.org/10.37750/2616-6798.2021.4(39).248794)
2. Солодка О. М. Забезпечення інформаційного суверенітету держави. *Інформація і право*. 2020. № 1 (32). С. 80–87. DOI: [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311)
3. Novikov Ye. Digital sovereignty: conceptual challenges and constitutional implications. *Конституційно-правові академічні студії*. 2024. № 1. С. 61–69. DOI: <https://doi.org/10.24144/2663-5399.2024.1.08>
4. Теорія держави і права. Академічний курс: підручник / за ред. О. В. Зайчука, Н. М. Оніщенко. Київ: Юрінком Інтер, 2006. 688 с.
5. Загальна теорія держави і права: підручник / М. В. Цвік, О. В. Петришин, Л. В. Авраменко та ін.; за ред. М. В. Цвіка, О. В. Петришина. Харків: Право, 2009. 584 с.
6. Бобровник С. В. Компроміс і конфлікт у праві: антрополого-комунікативний підхід до аналізу: монографія. Київ, 2011. 384 с.
7. Celeste E. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*. 2019. Vol. 33, No. 1. P. 76–99. DOI: <https://doi.org/10.1080/13600869.2019.1562604>
8. Daskal J. The Un-Territoriality of Data. *Yale Law Journal*. 2015. Vol. 125, № 2. P. 326–390.
9. Пархоменко Н. М. Джерела права: проблеми теорії та методології: монографія. Київ: Юридична думка, 2008. 336 с.
10. Cybersecurity Law of the People's Republic of China. URL: [https://www.dataguidance.com/sites/default/files/en\\_cybersecurity\\_law\\_of\\_the\\_peoples\\_republic\\_of\\_china\\_1.pdf](https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf) (дата звернення 18.02.2026).
11. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. 2016. URL: <https://www.legislation.gov.uk/eur/2016/679/contents> (дата звернення 18.02.2026).
12. European Commission. Shaping Europe's Digital Future. COM (2020) 67 final. Brussels, 2020. URL: [https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020\\_en\\_4.pdf](https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf) (дата звернення 18.02.2026).
13. Шевчук М. О. Аналіз національного законодавства про інформаційну безпеку. *Юридичний науковий електронний журнал*. 2025. № 1. С. 383–386. URL: [http://lsej.org.ua/1\\_2025/89.pdf](http://lsej.org.ua/1_2025/89.pdf) (дата звернення 18.02.2026). DOI: <https://doi.org/10.32782/2524-0374/2025-1/87>
14. Гусарєв С. Д., Тихомиров О. Д. Юридична деонтологія (основи юридичної діяльності): навч. посіб.; 3-тє вид., перероб. і доп. Київ: Знання, 2008. 495 с.
15. Радутний О. Е. Ілюзія та реальність інформаційного суверенітету. *Інформація і право*. 2020. № 4 (35). С. 22–38. DOI: [https://doi.org/10.37750/2616-6798.2020.4\(35\).221215](https://doi.org/10.37750/2616-6798.2020.4(35).221215)
16. Дзьобань О. П. Філософія інформаційних комунікацій: монографія. Харків: Майдан, 2012. 224 с.

17. Schmitt M. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017. 648 p.
18. Гічко О. В. Інформаційний суверенітет як передумова міжнародної співпраці України: питання захисту в умовах збройної агресії. *Науковий вісник Ужгородського національного університету*. Серія: ПРАВО. 2024. Вип. 86. Ч. 3. С. 272–277. DOI: <https://doi.org/10.24144/2307-3322.2024.86.3.41>
19. Куцепал С. В. Інформаційний суверенітет та інформаційна безпека України: виклики та реалії війни. *Полтавський правовий часопис*. 2023. № 1. С. 78–88. DOI: <https://doi.org/10.21564/2786-7811.1.290476>

## References

1. Ternavska V. M. Kontsepsiia derzhavnoho suverenitetu v aspekti hlobalnoho informatsiinoho prostoru. *Informatsiia i pravo*. 2021. № 4 (39). S. 80–89. DOI: [https://doi.org/10.37750/2616-6798.2021.4\(39\).248794](https://doi.org/10.37750/2616-6798.2021.4(39).248794) (in Ukr.).
2. Solodka O. M. Zabezpechennia informatsiinoho suverenitetu derzhavy. *Informatsiia i pravo*. 2020. № 1 (32). S. 80–87. DOI: [https://doi.org/10.37750/2616-6798.2020.1\(32\).200311](https://doi.org/10.37750/2616-6798.2020.1(32).200311) (in Ukr.).
3. Novikov Ye. Digital sovereignty: conceptual challenges and constitutional implications. *Konstytutsiino-pravovi akademichni studii*. 2024. № 1. S. 61–69. DOI: <https://doi.org/10.24144/2663-5399.2024.1.08> (in Ukr.).
4. Teoriia derzhavy i prava. Akademichniy kurs: pidruchnyk / za red. O. V. Zaichuka, N. M. Onishchenko. Kyiv: Yurinkom Inter, 2006. 688 s. (in Ukr.).
5. Zahalna teoriia derzhavy i prava: pidruchnyk / M. V. Tsvik, O. V. Petryshyn, L. V. Avramenko ta in.; za red. M. V. Tsvika, O. V. Petryshyna. Kharkiv: Pravo, 2009. 584 s. (in Ukr.).
6. Bobrovnyk S. V. Kompromis i konflikt u pravi: antropolocho-komunikatyvnyi pidkhid do analizu: monohrafiia. Kyiv, 2011. 384 s. (in Ukr.).
7. Celeste E. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*. 2019. Vol. 33, No. 1. P. 76–99. DOI: <https://doi.org/10.1080/13600869.2019.1562604>
8. Daskal J. The Un-Territoriality of Data. *Yale Law Journal*. 2015. Vol. 125, № 2. P. 326–390.
9. Parkhomenko N. M. Dzherela prava: problemy teorii ta metodolohii: monohrafiia. Kyiv: Yurydychna dumka, 2008. 336 s. (in Ukr.).
10. Cybersecurity Law of the Peoples Republic of China. URL: [https://www.dataguidance.com/sites/default/files/en\\_cybersecurity\\_law\\_of\\_the\\_peoples\\_republic\\_of\\_china\\_1.pdf](https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf) (data zvernennia 18.02.2026).
11. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. 2016. URL: <https://www.legislation.gov.uk/eur/2016/679/contents> (data zvernennia 18.02.2026).
12. European Commission. Shaping Europes Digital Future. COM (2020) 67 final. Brussels, 2020. URL: [https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020\\_en\\_4.pdf](https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf) (data zvernennia 18.02.2026).
13. Shevchuk M. O. Analiz natsionalnoho zakonodavstva pro informatsiinu bezpeku. *Yurydychnyi naukovyi elektronnyi zhurnal*. 2025. № 1. S. 383–386. URL: [http://lsej.org.ua/1\\_2025/89.pdf](http://lsej.org.ua/1_2025/89.pdf) (data zvernennia 18.02.2026). DOI: <https://doi.org/10.32782/2524-0374/2025-1/87> (in Ukr.).
14. Husariev S. D., Tykhomyrov O. D. Yurydychna deontolohiia (osnovy yurydychnoi diialnosti): navch. posib.; 3-tie vyd., pererob. i dop. Kyiv: Znannia, 2008. 495 s. (in Ukr.).
15. Radutnyi O. E. Iliuziia ta realnist informatsiinoho suverenitetu. *Informatsiia i pravo*. 2020. № 4 (35). S. 22–38. DOI: [https://doi.org/10.37750/2616-6798.2020.4\(35\).221215](https://doi.org/10.37750/2616-6798.2020.4(35).221215) (in Ukr.).
16. Dzoban O. P. Filosofiia informatsiinykh komunikatsii: monohrafiia. Kharkiv: Maidan, 2012. 224 s. (in Ukr.).
17. Schmitt M. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017. 598 p.
18. Hichko O. V. Informatsiinyi suverenitet yak peredumova mizhnarodnoi spivpratsi Ukrainy: pytannia zakhystu v umovakh zbroinoi ahresii. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia: PRAVO. 2024. Vyp. 86. Ch. 3. S. 272–277. DOI: <https://doi.org/10.24144/2307-3322.2024.86.3.41> (in Ukr.).
19. Kutsepал S. V. Informatsiinyi suverenitet ta informatsiina bezpeka Ukrainy: vyklyky ta realii viiny. *Poltavskiy pravoviy chasopys*. 2023. № 1. S. 78–88. DOI: <https://doi.org/10.21564/2786-7811.1.290476> (in Ukr.).

## Люлько С. А. Інформаційний суверенітет держави: структура і функції

Стаття присвячена теоретико-правовому аналізу структури та функцій інформаційного суверенітету держави в умовах глобальної цифровізації. Обґрунтовується позиція, що інформаційний суверенітет є функціональним виміром єдиного державного суверенітету в інформаційній сфері, а не його окремим видом. Виокремлено п'ять структурних компонентів: територіально-юрисдикційний, нормативно-правовий, технологічний, інформаційно-змістовий та міжнародно-правовий. Охарактеризовано захисну, регуляторну, розвиваючу, координаційну та міжнародно-представницьку функції. Обґрунтовується необхідність забезпечення

збалансованого розвитку всіх структурних компонентів інформаційного суверенітету держави та гармонійної реалізації всіх його функцій при дотриманні демократичних принципів.

*Ключові слова:* інформаційний суверенітет, цифровий суверенітет, структура, функції, кіберпростір, інформаційна безпека, правове регулювання, державне управління, Україна.

### **Liulko S. A. Information Sovereignty of the State: Structure and Functions**

The article provides a comprehensive theoretical and legal analysis of the structure and functions of state information sovereignty in the context of global digitalization. The nature of information sovereignty as a specific dimension of unified state sovereignty in the information sphere is examined. The plurality of approaches to defining information sovereignty in modern legal doctrine is analyzed, including works by leading Ukrainian and foreign scholars. The position is substantiated that information sovereignty is not a separate type of sovereignty but represents a functional manifestation of state sovereignty regarding the regulation of the information space.

Five structural components of information sovereignty are identified: territorial-jurisdictional (extension of state power to information processes occurring on state territory or concerning its citizens), normative-legal (legislative regulation system of the information sphere), technological (control over critical information infrastructure and development of national technologies), information-content (control over information content and ensuring information environment quality), and international-legal (participation in forming international rules of cyber behavior). These components form an integrated system whose effectiveness depends on balanced development of all elements. Different models of legal framework for information sovereignty are analyzed – Chinese (based on strict data localization and state security priority), European (balancing user rights protection and limitation of technological platforms dominance), American (sectoral regulation and free Internet principles), and Ukrainian (combining effective protection with democratic principles adherence).

The functional purpose of information sovereignty is characterized through five interrelated functions: protective (safeguarding national information space from external threats including cyberattacks and destructive information influences), regulatory (establishing rules for national information space functioning and technology standardization), developmental (creating conditions for national information and communication technologies development and digital economy growth), coordinational (harmonizing actions of various state bodies, private sector and civil society), and international-representative (participating in forming global Internet governance norms and protecting national interests globally).

The main problems and challenges of modern information sovereignty development are identified, including tension between state control aspiration and information freedom necessity, limitations of national regulation due to global nature of information flows, and regulatory gaps due to rapid technological changes. Special attention is paid to Ukrainian experience in forming an information sovereignty model under conditions of countering information aggression from the Russian Federation. Ukraine faces the unique challenge of simultaneously resisting large-scale information aggression while maintaining openness of information space, freedom of speech, and media pluralism. This requires a balanced model combining effective national interests protection with democratic standards compliance. The necessity of a systematic approach to developing all structural components is substantiated, as weakness of any single element undermines the state's overall capacity to protect its interests in the digital sphere and ensure national security. The article concludes that only harmonious realization of all identified functions – protective, regulatory, developmental, coordinational, and international-representative – ensures effective information sovereignty in the context of modern challenges including information aggression and European integration aspirations.

*Keywords:* information sovereignty, digital sovereignty, structure, functions, cyberspace, information security, legal regulation, public administration, Ukraine.

**DOI: 10.33663/2524-017X-2026-17-596-602**

Дата першого надходження рукопису до видання: 18.02.2026

Дата прийнятого до друку рукопису після рецензування: 09.04.2026

Дата публікації: 30.04.2026