

**Політологія**

**УДК 351.746.1:004.056.5**

**DOI** <https://doi.org/10.5281/zenodo.18233746>

**Взаємозв'язок між інформаційним суверенітетом і стійкістю держави до  
загроз нацбезпеці**

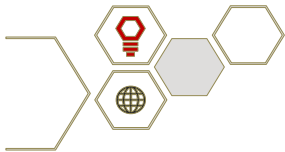
**Крап Андрій Павлович**

кандидат політичних наук, доцент кафедри права,  
Львівський інститут ПрАТ "ВНЗ "Міжрегіональна Академія управління  
персоналом, Київ, Україна, <https://orcid.org/0000-0002-4443-3364>

**Прийнято: 19.12.2025 | Опубліковано: 31.12.2025**

**Анотація:** Стаття присвячена комплексному аналізу та визначенню функціонального формату взаємозв'язку між інформаційним суверенітетом в умовах глобалізованого та віртуалізованого світу і стійкістю держави, що впливає із її здатності протистояти загрозам національній безпеці. Також метою статті було наголосити на важливості посилення національної системи кіберстійкості України в умовах повномасштабної війни та глобальної цифрової фрагментації.

Задля досягнення поставленої мети були використані системний підхід та методи порівняльного аналізу, щоб оглянути регуляторні механізми, зокрема, локалізації даних, на прикладі Китай та країн ЄС. Також було залучено досвід США. Концептуально-функціональний аналіз застосовано для операціоналізації поняття кіберстійкості та її залежності від політико-правового суверенітету держави. Геополітичний аналіз допоміг оглянути вплив анонімності кіберпорстору на ефективність/неефективність

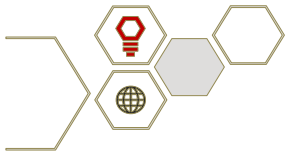


традиційних механізмів міжнародного права та ускладнення атрибуції кібератак.

У результатах дослідження підтверджено, що в умовах глобалізації та гібридної війни інформаційний суверенітет з теоретично концепту перейшов у розряд необхідної складової забезпечення стійкості держави, ставши частиною національної безпеки. Кіберстійкість є синергетичним результатом інтеграції правових захисних механізмів суверенітету та технічної спроможності держави. Важливим викликом залишається дилема пошуку балансу між суверенітетом та глобальної співдією. Зокрема, контроль над потоками даних, що вже застосовано у десятках країн, може призводити до фрагментації кіберпростору, здорожчання відповідних операційних заходів та обмеження доступу до міжнародних засобів кіберзахисту. Наголошено, що успішність протидії кіберзагрозам тісно пов'язана із гнучкістю правової системи держави, її адаптивністю до поточних і потенційних викликів та загроз та здатністю швидко на них реагувати.

Анонімність кіберпростору підриває основи традиційної моделі суверенітету, вимагаючи від держав, зокрема, й від України, нових дипломатичних та правових інструментів задля просування принципів відповідальності за кіберагресію.

Наукова новизна полягає в обґрунтуванні положення про те, що надмірна локалізація даних може призводити до фрагментації мережі та обмеження доступу до глобальних інструментів захисту. Аргументовано, що анонімність кіберпростору нівелює традиційні механізми міжнародного права, що вимагає впровадження нових інструментів юридичної атрибуції кібератак. Визначено пріоритети для України: формування людиноцентричної системи захисту даних (за моделлю ЄС) у поєднанні з гнучкими механізмами дипломатичної протидії кіберагресії. Обґрунтовано необхідність балансу між жорстким суверенним контролем (за прикладом КНР) та інтеграцією у глобальні безпекові структури.



У висновках наголошено на необхідності для України збалансованого підходу до формування захисту даних, зважаючи на досвід ЄС з акцентом на людиноцентричності та з активним просуванням інтересів України на міжнародній арені. При цьому необхідно зважати на вплив таких потужних гравців, як Китай, який демонструє значно більшу жорстку стратегію контролю свого інформаційного суверенітету та впливу на суверенітет інших держав і наддержавних структур. Важливим залишається міжнародне співробітництво у сфері вироблення правових механізмів інформаційного суверенітету як важливої складової національної безпеки.

**Ключові слова:** анонімність кіберпростору, безпека, глобалізація, держава, загрози, інформаційний суверенітет, кіберпростір, цифрова фрагментація, цифровізація економіки.

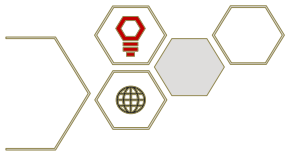
### **The relationship between information sovereignty and the state's resilience to national security threats**

**Andriy Krap,**

PhD in Polical Sciences, Associate Professor of the Department of Law,  
Lviv Institute of the Interregional Academy of Personnel Management  
Kyiv, Ukraine, <https://orcid.org/0000-0002-4443-3364>

**Abstract:** The article is devoted to a comprehensive analysis and definition of the functional format of the relationship between information sovereignty in the conditions of a globalized and virtualized world and the resilience of the state, which arises from its ability to resist threats to national security. The article also aimed to emphasize the importance of strengthening the national cyber resilience system of Ukraine in the conditions of a full-scale war and global digital fragmentation.

To achieve this goal, a systematic approach and comparative analysis methods were used to examine regulatory mechanisms, in particular, data localization, using

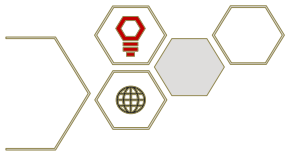


the example of China and EU countries. The experience of the USA was also involved. Conceptual and functional analysis was used to operationalize the concept of cyber resilience and its dependence on the political and legal sovereignty of the state. Geopolitical analysis helped to examine the impact of cyberspace anonymity on the effectiveness/inefficiency of traditional mechanisms of international law and the complication of attribution of cyberattacks.

The results of the study confirmed that in the context of globalization and hybrid warfare, information sovereignty has moved from a theoretical concept to a necessary component of ensuring the stability of the state, becoming part of national security. Cyber resilience is a synergistic result of the integration of legal protective mechanisms of sovereignty and the technical capabilities of the state. An important challenge remains the dilemma of finding a balance between sovereignty and global cooperation. In particular, control over data flows, which has already been applied in dozens of countries, can lead to fragmentation of cyberspace, increasing the cost of relevant operational measures and limiting access to international cyber defense tools. It is emphasized that the success of countering cyber threats is closely related to the flexibility of the state's legal system, its adaptability to current and potential challenges and threats, and the ability to respond quickly to them.

The anonymity of cyberspace undermines the foundations of the traditional model of sovereignty, requiring states, including Ukraine, to develop new diplomatic and legal instruments to promote the principles of responsibility for cyber aggression.

The scientific novelty lies in substantiating the position that excessive data localization can lead to network fragmentation and restricted access to global protection tools. It is argued that the anonymity of cyberspace nullifies traditional mechanisms of international law, which requires the introduction of new instruments of legal attribution of cyberattacks. Priorities for Ukraine are identified: the formation of a human-centric data protection system (based on the EU model) in combination with flexible mechanisms for diplomatic counteraction to cyber

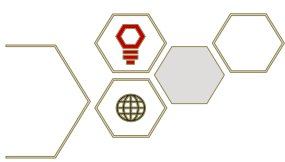


aggression. The need for a balance between strict sovereign control (following the example of the PRC) and integration into global security structures is substantiated.

The conclusions emphasize the need for Ukraine to adopt a balanced approach to the formation of data protection, taking into account the experience of the EU with an emphasis on human-centricity and with the active promotion of Ukraine's interests in the international arena. At the same time, it is necessary to take into account the influence of such powerful players as China, which demonstrates a much more rigid strategy of controlling its information sovereignty and influencing the sovereignty of other states and supranational structures. International cooperation in the development of legal mechanisms for information sovereignty as an important component of national security remains important.

**Keywords:** anonymity of cyberspace, security, globalization, state, threats, information sovereignty, cyberspace, digital fragmentation, digitalization of the economy.

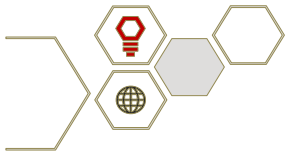
**Постановка проблеми.** Стрімке зростання ролі інформаційного суверенітету як на державному, так і на міжнародному рівні, а також загострення проблеми захисту приватності у віртуальному світі, чітко засвідчує, що очевидні переваги діджиталізації усіх сфер нашого життя мають і значний зворотний бік. Цей процес перетворив віртуальний простір на критично важливу сферу, де відтворюються всі форми суспільних та правовідносин, від електронних платежів та надання адміністративних послуг до електронного управління та правоохоронних функцій. Водночас, загрози національній безпеці та глобальній стабільності через кіберзлочинність та ворожу діяльність невпинно зростають. Як зазначено у Стратегії кібербезпеки України, сьогодні кіберпростір є невід'ємною частиною шостого технологічного укладу та офіційно визнаний театром воєнних дій. На тлі посилення геополітичного протистояння світових центрів сили, які прагнуть поділу сфер впливу, кіберзагрози стрімко зростають, формуючи нову



безпекову ситуацію. Основоположним джерелом загроз для України та міжнародної безпеки залишається РФ, яка активно застосовує концепцію інформаційного протиборства як поєднання деструктивних кібердій, кібертероризму та інформаційно-психологічних операцій у гібридній війні. З огляду на ці виклики, забезпечення кібербезпеки є пріоритетом національної безпеки України. Швидкозмінний цифровий світ вимагає від держави гнучкої, збалансованої та ефективної національної системи кібербезпеки, здатної стримувати деструктивні дії та досягати кіберстійкості на всіх рівнях [1].

В умовах повномасштабної агресії Росії проти України фактор віртуалізації набув специфічних рис, оскільки війна ведеться не лише на фізичному полі бою, але й активно в кіберпросторі. Це вимагає від держави формування потужної національної стійкості в інформаційній сфері. Невипадково забезпечення кібербезпеки визначено як один із пріоритетів у системі національної безпеки України. Отже, наукова проблема полягає у необхідності осмислення та визначення ключових механізмів, які забезпечують взаємозв'язок між інформаційним суверенітетом держави та її здатністю ефективно протистояти зростаючим кіберзагрозам національній безпеці в умовах гібридної війни. Забезпечення інформаційного суверенітету через ефективну інформаційну безпеку гарантує стабільність державних інститутів, збереження демократичних засад та національної ідентичності, що робить цей чинник у сучасній гібридній війні стратегічно не менш важливим, ніж військову чи економічну безпеку.

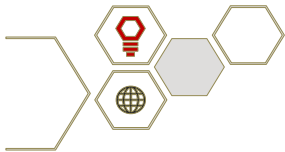
Гіпотеза дослідження ґрунтується на припущенні, що в умовах гібридної війни інформаційний суверенітет перестає бути інструментом ізоляції національного сегмента мережі, а натомість стає динамічним механізмом правової атрибуції загроз та адаптивного управління даними, що є визначальною умовою для формування стійкості держави перед обличчям повномасштабної кіберагресії.



**Аналіз останніх досліджень і публікацій.** Аналіз сучасної наукової думки дозволяє структурувати напрацювання за кількома ключовими векторами, що відображають трансформацію суверенітету в цифрову епоху.

Перша група досліджень фокусується на концептуалізації цифрового та інформаційного суверенітету як основи національної безпеки. Тематика статті передбачає охоплення кількох векторів наукових досліджень. Насамперед, йдеться про зацікавлення щодо самого поняття «інформаційний суверенітет» та його сутнісні характеристики. Особливо в умовах гібридних воєн та цифровізації усіх сфер життя. *L. Li* свою статтю присвятив проблемі суверенітету даних та національній безпеці в умовах стрімкого розвитку цифрової епохи. Автор сфокусовано досліджує дилеми та протиріччя, які виникають у процесі управління даними на міжнародному рівні. Дослідник запропонував звернути прискіпливу увагу на необхідність комплексного посилення законодавчої бази через зміцнення регуляторних норм і розвиток національних технологій захисту при активізації міжнародної співпраці й координації у сфері даних. Дослідження *L. Li* є важливим для розуміння того, як держави можуть сформувати ефективну стратегію збереження контролю над своїми даними та реагування на сучасні виклики в кіберпросторі [2].

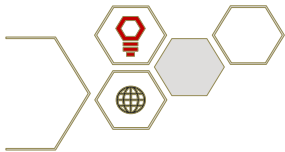
Другий напрям досліджень присвячений стійкості держави та викликам, що постають перед національними урядами. *C. Fjäder* аналізував трансформації ролі суверенних урядів у забезпеченні безпеки в умовах зростаючої складності та невизначеності глобального середовища. Він відзначив парадоксальну ситуацію: попит на безпеку зростає, тоді як можливості національних держав ефективно керувати цими викликами зменшуються. Дане дослідження мало на меті сприяти розвитку дискурсу навколо національної стійкості та допомогти у формуванні політик і практик, необхідних для встановлення послідовного стратегічного підходу до забезпечення національної стійкості [3].



*K. Yadav* вивчав виклики національному суверенітету та безпеці, спричинені взаємодією кіберпростору та державного суверенітету в цифрову епоху. Вкотре наголошено, що витoki даних, кібератаки та кібервійни стали реальними та значущими загрозами для економік, політики та територіальної цілісності більшості країн. Основний фокус у статті зосереджений на дослідженні механізмів, за допомогою яких кібербезпека перетинається з питаннями суверенітету [4]. *Y. Novikov* комплексно вивчав вплив технологічного суверенітету на економічну та національну безпеку. Автор продемонстрував його істотний, багатогранний вплив на загальну стабільність країни. Технологічний суверенітет є критичним чинником для трьох ключових сфер національної безпеки: економічна стабільність, енергетична та військова безпека [5].

Третій, найбільш релевантний для України вектор, охоплює питання інформаційної безпеки в умовах гібридної війни. *К. Ульяненко* досліджував інформаційну безпеку крізь призму національної стійкості України. Науковець особливу увагу приділив інформаційній безпеці як стрижню стійкості України та українців в умовах війни [6]. У статті *С. Куцепал* йде мова про інформаційний суверенітет та інформаційну безпеку України в контексті військової агресії РФ. Авторка визначає національну безпеку як «інформаційний фронт», де інформаційний суверенітет є ключовою умовою стійкості. Аргументовано, що інформаційна безпека займає центральне місце в системі нацбезпеки, забезпечуючи захист від негативного інформаційного впливу ворога та доступ до достовірних даних [7]. Правові аспекти поняття «інформаційний суверенітет», його тлумачення та підходи до практичної реалізації відображені у публікаціях *О. Солодки* та *О. Довганя* [8; 9].

Проблемам державного суверенітету у контексті економічного розвитку присвячене дослідження *І. Дробуш, Л. Корнути, М. Українця* [10]. *В. Тернавська* зробила огляд концепції державного суверенітету крізь призму глобального розвитку [11]. Різноманітним аспектам інформаційної безпеки

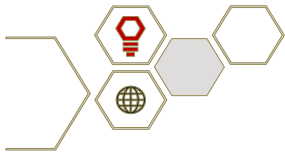


присвячені наукові напрацювання *В. Шемчука* [12], *О. Звездової*, *О. Вакалюка* [13], *Н. Хомі* [14]. Вплив ІІІ на національну безпеку став предметом аналізу у публікаціях *М. Mansur* [15], *К. Srivastava* [16].

Виокремлені підходи свідчать, що інформаційний суверенітет трансформувався з теоретичної категорії у практичний інструмент забезпечення стійкості держави. Водночас динаміка розвитку технологій та специфіка повномасштабної агресії зумовлюють необхідність подальшого поглиблення аналізу взаємозв'язку між суверенним контролем над даними та адаптивною кіберстійкістю.

Навіть побіжний огляд наукових напрацювань свідчить про важливість інформаційного суверенітету в умовах глобалізації як одну із підвалин стійкості держави та її національної безпеки. Окрім того, зважаючи на динаміку розвитку інформаційних технологій, дана тема ще довго не втратить наукової та практичної значущості.

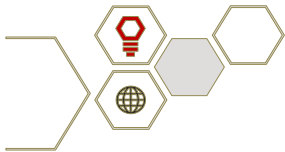
**Виділення невирішених раніше частин загальної проблеми.** Попри значний обсяг наукових праць, присвячених вивченню інформаційного суверенітету та його сутнісних характеристик як складової стійкості держави в умовах кризових ситуацій, наразі низка важливих аспектів проблематики дослідження залишається маловивченою або поза увагою науковців. Наразі важливо зосередити дослідницьку увагу на концептуалізації кіберстійкості у сучасних вимірах державного суверенітету. Стратегічної ваги такі дослідження набувають в умовах зростаючих воєнних загроз, особливо загроз кібервійни. Окрім того, скрупульозного аналізу потребують наслідки впливу позатериторіальних впливів регуляторних ініціатив на суверенні права держави у кіберпросторі. Важливою науковою і практичною проблемою залишається правовий бік розвитку інформаційних технологій та їх впливу на національну і глобальну безпеку. Потребує уваги й осмислення балансу між суверенітетом та глобальною співпрацею, наприклад, у сфері торгівлі, що



безпосередньо впливає на економічну стійкість держави та захищеність її громадян через захист її даних у кіберпросторі.

Попри значний обсяг наукових праць, присвячених інформаційному суверенітету як складовій стійкості держави, низка аспектів залишається маловивченою, що зумовлює структуру даного дослідження. Йдеться про концептуалізація кіберстійкості. Потребує уточнення саме функціональний взаємозв'язок між технічною стійкістю та політико-правовим суверенітетом, особливо в умовах кібервійни. Необхідно проаналізувати транскордонний вплив регуляцій. Скрупульозного аналізу потребують наслідки впливу позатериторіальних регуляторних ініціатив на суверенні права держав. Цей аспект досліджується у статті на прикладі порівняння правових стратегій локалізації даних у США, КНР та ЄС. Залишається відкритою проблема адаптації міжнародного права до викликів анонімності та складності атрибуції кібератак. Зазначену прогалину заповнено шляхом аналізу ефективності традиційних правових механізмів у віртуалізованому середовищі. Потребує осмислення баланс між захистом національного сегмента мережі та участю у глобальних економічних і безпекових процесах. Цей баланс виведено у висновках статті як рекомендацію щодо формування гнучкої моделі національної системи кібербезпеки України. Саме такий підхід дозволяє комплексно підійти до розв'язання наукової проблеми та обґрунтувати пропоновані стратегічні пріоритети для зміцнення національної стійкості.

**Формулювання цілей статті (постановка завдання).** Оскільки значна кількість досліджень проходила або у мирний час, або базуючись на даних без врахування викликів та загроз війни, то не була врахована специфіка повномасштабної війни, яка охоплює як фізичний, так і віртуальний вимір. Тобто, коли кіберпростір став повноцінним театром бойових дій. Також існує розрив між дослідженнями в галузі права, що більше уваги звертають на правові аспекти суверенітету, та дослідженнями в галузі кібербезпеки, що більше зважають на проблеми стійкості і можливі загрози та їх перебіг і

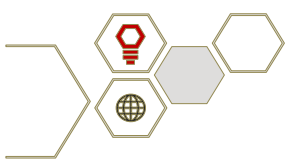


наслідки. Тому метою статті є проаналізувати еволюцію інформаційного суверенітету та розуміння поняття стійкості держави крізь призму їх взаємозв'язку для національної безпеки.

### **Виклад основного матеріалу дослідження.**

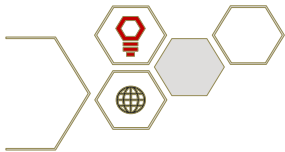
Для досягнення поставленої мети та забезпечення об'єктивності результатів у статті використано комплекс загальнонаукових та спеціальних методів. Системний підхід застосовано для аналізу інформаційного суверенітету як багаторівневої системи, що інтегрована в загальну структуру національної безпеки. Компаративістський метод використано при дослідженні регуляторних моделей США, КНР та країн ЄС, що дозволило виявити особливості національних стратегій локалізації даних та захисту кіберпростору. Концептуально-функціональний аналіз слугував основою для операціоналізації поняття «кіберстійкість» та визначення його залежності від політико-правового статусу держави. Геополітичний та прогностичний методи дали змогу оцінити вплив анонімності віртуального простору на трансформацію міжнародного права та спрогнозувати ризики цифрової фрагментації для України.

Зазвичай поняття «суверенітет держави» трактується у межах політико-правових категорій для демонстрації сутності обсягу можливостей та компетенції держави у її внутрішній та зовнішній політичній діяльності. Факт появи певної держави автоматично передбачав її суверенітет. При цьому, втрата державного суверенітету означає припинення її функціонування як суб'єкта міжнародного права, тому що суверенітет є прерогативою держави. Але варто все-таки уникати абсолютизації державного суверенітету як сталої величини, оскільки йому не є притаманним абсолютний характер. Посилення глобалізаційних процесів, зростання впливу кіберпростору на геополітику та геоекономіку і міжнародну безпеку стимулюють посилення контактів та зближення позицій різних держав. Формування різноманітних ситуативних союзів або довготривалих альянсів. Так, наприклад у часи Холодної війни,



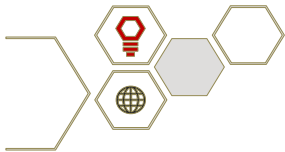
попри формальне визнання суверенітету, більшість тогочасних держав світу були у сфері впливу або США, або СРСР. Кардинальні геополітичні зміни кінця ХХ ст. зумовили й необхідність переосмислення державного суверенітету та формування нових теоретичних і практичних підходів до світоустрою. Економічна взаємозалежність та зростання впливу наднаціональних структур (Європейський Союз, Міжнародний валютний фонд, Світовий банк тощо) поставили на порядок денний важливість трансформування державного суверенітету, зважаючи на зміну «правил гри» у геополітиці. Зокрема, у країнах Європи питання національного суверенітету є предметом інтенсивних дискусій у контексті євроінтеграції. Європейський Союз передбачає передачу частини суверенітету держав-членів у певних сферах, що принесло значні економічні та політичні вигоди. Водночас, зберігається постійне занепокоєння щодо втрати національного суверенітету та проблеми демократичного дефіциту європейських інституцій. Європейські країни демонструють різні підходи: одні акцентують увагу на національній незалежності, тоді як інші більш готові до спільного суверенітету в межах ЄС [17, р. 257].

Ухвалення статуту ООН у 1945 р. базувалося як на тогочасних геополітичних реаліях, так і спиралося на наукові напрацювання щодо суверенітету та його характеристик. Зокрема, В. Fassbender слушно називає ці процеси переломним етапом у розвитку міжнародних відносин і права. Дослідник визначає суверенну сутність держав як конституційну автономію у міжнародно-правовому порядку. Така автономія гарантує державі рівний статус у межах конституції міжнародної спільноти. Таким чином формується право на захист цієї автономії та право на участь у міжнародному співтоваристві [18, р. 1632]. Попри те, що формальні дефініції суверенітету містять перелік суттєвих його характеристик, це все-таки висуває на перший план питання про сучасний зміст державного суверенітету. Свого часу ще філософ та правник Ж. Боден сформулював характерні ознаки суверенітету,



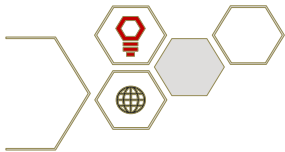
насамперед, виключне право держави на законодавчу діяльність щодо своїх суб'єктів. До них з плином часу додалися й такі, як: територіальний контроль з монополією на легітимний примус; контроль над грошово масою та грошовими потоками та встановлення і стягнення податків; оприлюднення законів та здійснення кримінального правосуддя; право на оголошення війни; ведення переговорів на міжнародному рівні; делегування представників до міжнародних структур та організацій; повноваження щодо надання громадянства та захисту. Тобто, попри процес релятивізації та обмеження державного суверенітету з середини ХХ ст., його фундаментальні засади залишаються ідентифікованими та зберігають свою практичну значущість [18 р. 1632].

У сучасних геополітичних умовах державний суверенітет перестає бути абсолютною та неподільною категорією, трансформуючись у переговорний концепт, обумовлений глобальними взаємозалежностями та необхідністю міжнародного співробітництва. Хоча національні держави зберігають свій статус індивідуальних акторів на міжнародній арені, вони змушені здійснювати суверенітет з урахуванням складних реалій сучасного світу. Динамічний технологічний розвиток у ХХІ ст., перехід до цифрового суспільства, зумовили й необхідність до вироблення розуміння територіальних меж суверенних держав в інформаційному просторі, зокрема, й з врахуванням питань національної безпеки. Очевидно, що кіберпростір не корелює з географічними кордонами та межами, які були покладені в основу ще Вестфальської системи. Як зазначає В. Тернавська, ще у другій половині ХХ ст. була розроблена концепція інформаційного суверенітету. Її поява була зумовлена з космічними програмами, зокрема, із запуском першого штучного супутника Землі. Такий стрибок у сфері комунікацій та науково-технічного розвитку призвів й до потреби увиразнення таких змін у міжнародних відносинах, що є предметом теоретичних та практичних напрацювань й по сьогодні. Розвиток інформаційного суспільства та формування нових



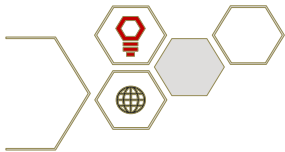
глобальних механізмів врядування та архітектури національної безпеки, міжнародна співпраця у сфері безпеки стали можливими завдяки саме розвитку технологій Інтернету. Інтеграція сучасних інформаційних технологій створює умови для виникнення локальних та національних кіберфізичних систем, що передбачають імплементацію елементів штучного інтелекту (ШІ) в процеси управління. При цьому загострюються проблеми несанкціонованого поширення інформації, втручання іноземних держав у виборчі процеси, фальсифікації результатів референдумів, кібератак на інформаційні бази даних національних систем управління та інформаційний тероризм. Недостатній рівень захищеності інформаційних ресурсів призводить до витоку критично важливої інформації політичного, економічного, науково-технічного чи оборонного характеру, що становить сутність національних інтересів. Це стимулює уряди США, Великої Британії, Китаю та держав-лідерів ЄС до активного формування нової інформаційної політики. Наприклад, у США значна шкода національній безпеці та економіці внаслідок злочинних дій недержавних структур (терористичних угруповань), а також кібератак з боку РФ, Ірану та Північної Кореї, а також економічного шпигунства з боку КНР, стала підставою для ухвалення Національної кіберстратегії США 2018 р., спрямованої на зміцнення національної кібербезпеки [11, с. 80-81].

Початок ХХІ ст. став й тим часом в історії людства, коли поширення цифрових технологій суттєво трансформувало глобальний світ, поклавши початок небачених досі взаємозв'язків, креативності та можливостей. Водночас, бачимо й вразливі місця таких стрімких змін. У контексті України вони особливо гостро увиразнюються в умовах війни. Очевидно, що війна є руйнівною подією, яка підриває економіку та й загалом інституційні основи держави. Суттєвої ваги набувають такі параметри державної стійкості, як здатність до швидкої мобілізації комунікаційних ресурсів; забезпечення безперервності управління, в тому числі й у кіберпросторі; правова гнучкість й адаптивність для реагування на інформаційні виклики та збереження



суспільної довіри до державних інституцій. Ослаблення вказаних чинників підриває інформаційний суверенітет держави, що підвищує ризик втрати стратегічної автономії, економічної стабільності і, в критичних випадках, національного суверенітету загалом. Повномасштабна війна росії проти України продемонструвала, поміж іншого, що інституційна стійкість держави є не лише політичною чи економічною, а й критичною категорією національної безпеки. Стійкість у цьому контексті виходить за межі простого виживання державних структур, охоплюючи їхню здатність до адаптації, збереження легітимності та забезпечення ефективного управління в умовах екстремального стресу. Український досвід підтверджує, що стійкість слугує вирішальним мостом між політичною стабільністю, суспільною довірою та економічною/інформаційною безпекою [19, р. 266].

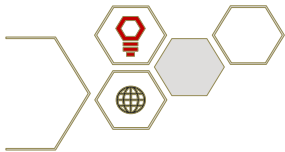
Стійкість держави історично пов'язували із її військовим потенціалом. Однак на сьогодні його розширено й за рахунок політико-психологічних аспектів. У сучасному розумінні стійкість вже не є просто здатністю до виживання. Йдеться про комплексну спроможність суспільства протистояти широкому спектру криз, від стихійних лих до подій, пов'язаних із національною безпекою, як-от війни чи терористичні атаки. Чинниками такої стійкості є впровадження змін і адаптацій без шкоди для основних цінностей та інститутів суспільства. Також, говорячи про стійкість держави, важливо враховувати здатність нації успішно долати труднощі, як-от бідність, корупція чи тероризм, зберігаючи при цьому свою соціальну тканину цілісною. Хоча стійкість й виходить за межі лише військового виміру, вона набула особливої актуальності саме в умовах посилення турбулентності у міжнародних відносинах та загострення протистояння між геополітичними гравцями. Зокрема, напруга в Індो-Тихоокеанському, Близькосхідному регіонах та, особливо, повномасштабна російсько-українська війна стали каталізаторами інтересу до стійкості держави. У часи глобальної нестабільності вона випробовується низкою загроз: міграційні кризи, кліматичні катаклізми,



підривання енергетичної безпеки. Йдеться також про виклики, зумовлені цифровізацією, кібертероризмом та ІІІ. Зазначені загрози безпосередньо стосуються інформаційного суверенітету держави як фактору національної безпеки [14, с. 120-121].

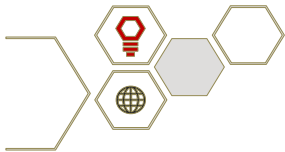
Кіберпростір є водночас масштабним, комплексним та критично важливим середовищем, де формується значна частина сучасних загроз національній безпеці. Ландшафт кіберзагроз характеризується високою диверсифікацією суб'єктів та їхніх можливостей. Він охоплює широкий спектр акторів з різною мотивацією. Серед них є як індивідуальні хакери, так і розгалужені та добре інститутовані і фінансовані терористичні організації з висококваліфікованими фахівцями у сфері ІТ-технологій [20]. Національні держави також використовують можливості кіберпростору як інструмент гібридної агресії. Проблема, яка безпосередньо впливає на здатність держави захищати свій інформаційний суверенітет, полягає у властивостях самого Інтернету. Анонімність і повсюдність мережі дозволяють зловмисникам діяти з високим ступенем секретності та безкарності. Така анонімність ускладнює атрибуцію атак та оперативне реагування, ставлячи під сумнів ефективність традиційних механізмів міжнародного права у цій сфері. Зростаюча залежність суспільства від цифрових технологій не лише багаторазово посилила занепокоєння щодо кібербезпеки, але й вивела на перший план стратегічне питання цифрового суверенітету. У міру того як держави прагнуть захистити свою критичну цифрову інфраструктуру та особисті дані громадян, вони водночас стверджують своє невід'ємне право контролювати й регулювати цифровий простір у межах своїх національних юрисдикцій [21].

У відповідь на зростаючий міжнародний тиск, що походить від домінуючої ролі глобальних технологічних корпорацій та множинних загроз кібербезпеці, багато країн активно розробляють політику та стратегії, спрямовані на підвищення їхнього цифрового суверенітету. Напрямки розвитку передбачають зростання рівня цифрової компетенції; локалізація



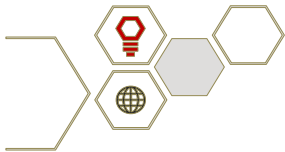
збереження та обробки даних у межах державних кордонів; обмеження потоку даних. Зокрема, станом на 2023 р. 100 обмежувальних заходів діяло на території 40 країн. Понад 2/3 з них поєднували вимоги щодо місцевого зберігання із заборonoю транскордонних потоків. З огляду на зростання кількості обмежувальних заходів локалізації даних (таких як обов'язкове місцеве зберігання і заборона транскордонного потоку), які підвищують операційні витрати та кібербезпекові ризики, актуальним є постійний моніторинг наслідків для економічної та цифрової стійкості. Цей моніторинг має стати основою для узгодження глобальних правил і стандартів щодо обробки та зберігання даних. Міжнародні зусилля повинні бути спрямовані на створення системи, яка б забезпечувала легітимні національні цілі, водночас запобігаючи надмірній фрагментації світового кіберпростору та збереженню переваг цифрової економіки [22, р. 1].

Світові гравці у нинішніх умовах обирають різні стратегії інформаційного суверенітету. Наприклад, Китай зупинився на жорсткому форматі кіберсуверенітету. Він передбачає суворий контроль над внутрішнім Інтернет-простором, активний розвиток вітчизняних технологічних компаній та запровадження національних стандартів і протоколів щодо кіберпростору та його використання. Підхід Китаю до ретериторіалізації кіберпростору є загальновідомим. Однак необхідно відзначити значно важливішу тенденцію: розширення регуляторної влади Китаю за межі його національної території. Це свідчить про формування просторово експансивного та наступального розуміння китайського цифрового суверенітету. Зокрема, W. Cong, проаналізувавши законодавчі ініціативи Китаю у сфері освоєння кіберпростору, наголошує на двох основних підходах Китаю до розширення цифрового виміру свого суверенітету. По-перше, йдеться до мінливості геостратегічних інтересів Пекіну. І даний підхід є контрастним, порівняно з відповідними практиками США та ЄС, хоча й має місце наслідування регуляторних механізмів. Однак, як наголошує дослідник, ця тенденція до



екстериторіальності неминуче зіткнеться зі значними концептуальними та практичними викликами у міжнародному правовому полі. По-друге, вказується на блокування або протидію з боку Китаю іноземних заходам, які вважаються обмежувальними або дискримінаційними щодо Китаю [23].

Якщо вести мову про країни Європейського Союзу, то у ЄС основними важелями вироблення правових механізмів забезпечення і контролю інформаційного суверенітету з акцентом на людиноцентричному підході. Зважаючи на зростання глобальної цифрової конкуренції, ЄС. Посилює свій курс на досягнення цифрового або технологічного суверенітету. Така політика стала відповіддю на занепокоєння, що громадяни, а також бізнес і держави-член ЄС поступово, але невпинно, втрачають контроль над своїми даними та інноваційним потенціалом. Але найважливіше, що втрачається й здатність дотримання законодавству у цифровому просторі. Політичний, соціальний та економічний вплив технологічних компаній-гігантів, які не є частиною ЄС, є загрозою для громадян щодо збереження персональних даних та обмежують розвиток європейських високотехнологічних компаній. Тому для ЄС цифровий суверенітет визначається як здатність діяти незалежно у цифровому світі. Така концепція включає два взаємодоповнюючі виміри. З одного боку, йдеться про захисні механізми, які передбачають захист даних, кібербезпеку та впровадження етичних стандартів. Останній пункт особливо посилюється з появою та широким застосуванням ШІ. З іншого, необхідним є стимулювання власних цифрових інновацій та забезпечення європейського лідерства у цій галузі. Президентка Європейської Комісії Урсула фон дер Ляєн зробила досягнення технологічного суверенітету у критичних сферах ключовим пріоритетом, особливо наголошуючи на проблемі конкуренції з боку глобальних гравців, які не завжди дотримуються європейських правил та основоположних цінностей. Також пандемія COVID-19 прискорила осмислення необхідності суверенних цифрових технологій, підтвердивши критичну роль високотехнологічного сектору для безперервності соціального



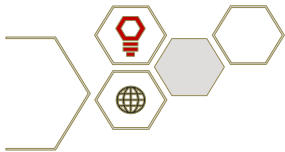
та економічного життя. Європейська Рада закликала до стратегічної автономії ЄС у постпандемічному контексті, наголошуючи на інвестиціях у цифрову інфраструктуру та технології. Регуляторні акценти ЄС передбачають зменшення залежності від зовнішніх технологічних постачальників, особливо на тлі занепокоєння щодо китайської технологічної присутності. Йдеться й про приділення особливої уваги безпеці даних та етичному регулюванню ШІ. Таким чином, політика ЄС спрямована на оновлення правових та фінансових інструментів для проактивного просування європейських цінностей і закріплення стратегічної автономії у цифровій сфері [24].

На прикладі Китаю та ЄС ми бачимо, що, незалежно від обраної стратегії, зміцнення національного (чи наднаціонального) контролю над цифровим простором є вже dokonаним фактом та пріоритетом задля збереження державної стійкості та національної безпеки.

**Висновки.** На основі проведеного аналізу з'ясовано, що в умовах гібридної війни інформаційний суверенітет вже не можна розглядати лише як політико-правову категорію. Він перейшов у розряд критичної операційної умови для забезпечення інституційної стійкості держави та забезпечення її суб'єктності в умовах воєнних загроз і викликів. Зокрема, досвід України після 2022 р. демонструє, наскільки стійкість держави, її інституцій та суспільства, є необхідною ланкою між політичною стабільністю, суспільною довірою та інформаційною безпекою.

Також встановлено, що кіберстійкість держави є результатом інтеграції правових захисних механізмів суверенітету та технічної спроможності. Наголошено, що успішність протидії гібридній агресії залежить від гнучкості правової системи та її здатності швидко реагувати на нетрадиційні загрози, які виникають через анонімність кіберпростору та його швидкості й динамізму.

Водночас залишається актуальною дилема фрагментації та локалізації. Заходи, пов'язані із локалізацією даних, хоча й посилюють, а то й монополізують державний контроль, мають ризики економічної фрагментації



та підвищення операційних витрат. Тому для України важливо розробити збалансований підхід, зосередившись на локалізації даних, які є важливими для національної безпеки, але при цьому зберігати відкритість для міжнародної цифрової економіки.

Не втрачає актуальності необхідність посилення міжнародної взаємодії у сфері атрибуції кібератак та активного використання міжнародних платформ та структур задля просування інтересів України щодо відповідальності країни-агресорки росії у кіберпросторі.

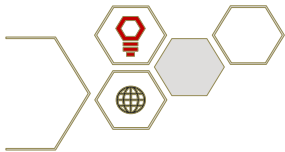
Подальше зміцнення кіберстійкості має ґрунтуватися на моніторингу балансу між суверенітетом і цифровою інтеграцією, що має забезпечити стратегічну технологічну і інформаційну автономію як важливий чинник стійкості держави в умовах глобалізації та динамічного технологічного розвитку.

Пропонується у державній політиці щодо кіберзахисту впровадження моделі гнучкого суверенітету, що передбачає створення національної платформи юридичної атрибуції кіберінцидентів у поєднанні із законодавчим закріпленням механізмів динамічного управління потоками даних. Це дозволить забезпечити стратегічну інформаційну автономію України без ризику технологічної ізоляції, інтегруючи вітчизняну систему кібербезпеки у глобальні безпекові структури як рівноправного та стійкого суб'єкта.

Подальші дослідження мають бути зосереджені на моніторингу балансу між суверенітетом і цифровою інтеграцією в контексті розвитку штучного інтелекту та його впливу на національну безпеку.

### Список використаних джерел

1. Наказ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»» (2021). *Президент України. Офіційне Інтернет-представництво*. URL: <https://www.president.gov.ua/documents/6852021-41069>



2. Li L. Data Sovereignty and National Security: Governance Challenges and Pathways in the Digital Ag. *Global Review of Humanities, Arts, and Society (GRHAS)*, 2025. Volume 1. № 1. P. 49-58. DOI: <https://doi.org/10.63802/grhas.v1.i1.7>

[https://www.researchgate.net/publication/391382001\\_Data\\_Sovereignty\\_and\\_National\\_Security\\_Governance\\_Challenges\\_and\\_Pathways\\_in\\_the\\_Digital\\_Age](https://www.researchgate.net/publication/391382001_Data_Sovereignty_and_National_Security_Governance_Challenges_and_Pathways_in_the_Digital_Age)

3. Fjäder C. The nation-state, national security and resilience in the age of globalisation. *Resilience*, 2014. Volume 2 (2). P. 114–129. DOI: <https://doi.org/10.1080/21693293.2014.914771> URL: <https://www.tandfonline.com/doi/full/10.1080/21693293.2014.914771>

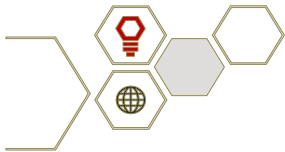
4. Yadav K. Cybersecurity and National Sovereignty: Challenges in the Digital Age. *International Journal of Social Science Research (IJSSR)*, 2024. Volume 1. Issue 1. P. 1-14. URL: <https://www.ijssr.com/>

5. Novikov Y. Technological sovereignty of the state: Practical experience of Ukraine and the European Union. *Philosophy, Economics and Law Review*, 2024. Volume 4. No. 2. P. 16-35. DOI: <https://doi.org/10.63341/2786-491X-2024-2-16> URL: <https://phelr.com.ua/en/journals/tom-4-2-2024/tekhnologichny-suverenitet-derzhavi-praktichny-dosvid-ukrayini-ta-yevropeyskogo-soyuzu>

6. Ульяненко К. Інформаційна безпека як фактор формування національної стійкості України. *Політикус*, 2025. Випуск 2. С. 148-153. DOI: <https://doi.org/10.24195/2414-9616.2025-2.23>

7. Куцепал С. 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> <https://plr.nlu.edu.ua/article/view/290476>

8. Солодка О. Забезпечення інформаційного суверенітету держави: правовий дискурс. *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) URL:



<https://ippi.org.ua/solodka-om-zabezpechennya-informatsiinogo-suverenitetu-derzhavi-pravovii-diskurs-st-80-87>

9. Довгань О. Національний інформаційний суверенітет – об’єкт інформаційної безпеки. *Інформація і право*, 2014. № 3 (12). С. 102-112. DOI: [https://doi.org/10.37750/2616-6798.2014.3\(12\).272574](https://doi.org/10.37750/2616-6798.2014.3(12).272574) URL: <https://www.ippi.org.ua/dovgan-od-natsionalnii-informatsiinii-suverenitet-%E2%80%93-ob%E2%80%99%D1%94kt-informatsiinoi-bezpeki>

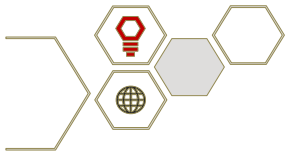
10. Drobush I., Kornuta L., Ukrainets M. (2025). Ensuring state sovereignty as a guarantee of the country’s economic development. *Baltic Journal of Economic Studies*, 2025. № 11(3). P. 212-221. DOI: <https://doi.org/10.30525/2256-0742/2025-11-3-212-221> URL: <http://www.baltijapublishing.lv/index.php/issue/article/view/2961>

11. Тернавська В. 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) URL: <http://il.ippi.org.ua/article/view/248794>

12. Шемчук В. *Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз*. Київ: Видавництво Ліра-К, 2020. 352 с.

13. Звездова О., Вакалюк О. Стратегія забезпечення кібербезпеки в гібридній війні. *Acta de Historia & Politica: Saeculum XXI*, 2021-2022. № 3. С. 82-90. DOI: <https://doi.org/10.26693/ahpsxxi2021-2022.03.082> URL: [https://www.researchgate.net/publication/361959366\\_Strategia\\_zabezpecenna\\_kiberbezpeki\\_v\\_gibridnij\\_vijni](https://www.researchgate.net/publication/361959366_Strategia_zabezpecenna_kiberbezpeki_v_gibridnij_vijni)

14. Хома Н. Національна стійкість: зміст та стратегія забезпечення в умовах війни та повоєнного відновлення. *Вісник Маріупольського державного університету. Серія: Історія. Політологія*, 2024. Випуск 38. С. 119-128. DOI: <https://doi.org/10.34079/2226-2830-2024-14-38-119-128> URL: <https://visnyk.mu.edu.ua/index.php/politologia/article/view/186/182>



15.Mansur M. National Security and Cyber Defense in the Rise of Artificial Super Intelligence. *European Scientific Journal, ESJ*, 2025. № 39. P. 32-329. DOI: <http://10.19044/esipreprint.3.2025.p320> URL:

<https://eujournal.org/index.php/esj/article/view/19248>

16.Srivastava K. Artificial intelligence and national security: perspective of the global south. *International Journal of Law in Changing World*, 2023. № 2. P. 77-87. DOI: <https://doi.org/10.54934/ijlcw.v2i2.6310> URL:

[https://www.researchgate.net/publication/376949864\\_ARTIFICIAL\\_INTELLIGENCE\\_AND\\_NATIONAL\\_SECURITY\\_PERSPECTIVE\\_OF\\_THE\\_GLOBAL\\_SOUTH](https://www.researchgate.net/publication/376949864_ARTIFICIAL_INTELLIGENCE_AND_NATIONAL_SECURITY_PERSPECTIVE_OF_THE_GLOBAL_SOUTH)

17.Goleanu C. E. Some Aspects of National Sovereignty in the International Geopolitical Context. *Interdisciplinary Journal of Research and Development*, 2025. Volume 12. № 1. P. 256-265. DOI: <https://doi.org/10.56345/ijrdv12n1s134> URL:

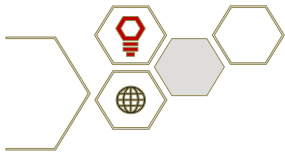
[https://www.researchgate.net/publication/394071430\\_Some\\_Aspects\\_of\\_National\\_Sovereignty\\_in\\_the\\_International\\_Geopolitical\\_Context](https://www.researchgate.net/publication/394071430_Some_Aspects_of_National_Sovereignty_in_the_International_Geopolitical_Context)

18.Fassbender B. Are the EU Member States Still Sovereign States? The Perspective of International Law. *European Papers*, 2023. Volume 8. No 3. P. 1629-1643. DOI: <https://doi.org/10.15166/2499-8249/733> URL: <https://www.europeanpapers.eu/e-journal/are-eu-member-states-still-sovereign-states-perspective-international-law>

19.Pustovar, Zakharenko, Minenko, Institutional stability of the state during the war political factors of economic security of Ukraine. *Baltic Journal of Economic Studies*, 2025. Volume 11. No. 4. P. 260-268. DOI: <https://doi.org/10.30525/2256-0742/2025-11-4-260-268> URL:

<http://www.baltijapublishing.lv/index.php/issue/article/view/3037/3009>

20.Balarabe K. Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. *Computer Law & Security*



*Review*, 2025. Volume 58. DOI: <https://doi.org/10.1016/j.clsr.2025.106180> URL: <https://www.sciencedirect.com/science/article/abs/pii/S2212473X25000537>

21. Stummer S. A Right to Anonymity in the Digital Age. A Discussion of the Opportunities, Risks and Limitations. *Verfassungblog*, 02 December 2024. URL: <https://verfassungsblog.de/a-right-to-anonymity-in-the-digital-age/>

22. Giovane C. D., Ferencz J., López-González J. *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD trade policy paper N°278. OECD 2023. 33 p. URL: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures\\_249df37e/179f718a-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf)

23. Cong W. The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics. In: Jiang M, Belli L, eds. *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Communication, Society and Politics*. Cambridge University Press; 2025. P. 63-80. URL: <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/spatial-expansion-of-chinas-digital-sovereignty/D18D59288E33063AF1EBAF416FACD6A2>

24. Madiega T. *Briefing EPRS Ideas Paper Towards a more resilient EU*. European Parliamentary Research Service. PE 651.992 - July 2020. 12 p. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)