УДК 342.95 (477)
DOI https://doi.org/10.32782/klj/2021.4.28

Зубко О. М.,
здобувач наукового ступеня доктора юридичних наук
Науково-дослідного інституту публічного права

КІБЕРСУВЕРЕНІТЕТ ЯК НОВА КАТЕГОРІЯ В АДМІНІСТРАТИВНОМУ ПРАВІ

Анотація. Актуальність статті полягає в тому, що в сьогоднішньому глобалізованому світі інформація й бази даних є тими унікальними ресурсами, без використання та збереження яких неможливе як існування й розвиток сучасної держави як суспільно-політичного утворення, так і виконання суто військових завдань щодо збереження незалежності та захисту країни. На думку експертних кіл та аналітиків провідних країн світу, гібридність сучасного збройного конфлікту визначається саме наявністю потужної інформаційного й кібернетичного складника. Мета статті полягає в тому, щоб на основі системного аналізу позицій учених, довідникових матеріалів і норм чинного законодавства розкрити кіберсуверенітет як нову категорію в адміністративному праві. Наголошено, що в міру свого розвитку Інтернет поступово став життєво необхідною інфраструктурою для всіх країн світу. Останнім часом у різних країнах виникають питання, пов'язані з кібербезпекою, і держави всього світу почали створювати власні системи кібербезпеки. Кіберсуверенітет є природним продовженням національного суверенітету. Для відповіді на ці виклики необхідно вивчити майбутнє кібербезпеки для країн, що розвиваються. Жодна держава не здатна домогтися абсолютної безпеки. Підкреслена повага до кіберсуверенітету не означає відключення Інтернету й ізоляції країни від зовнішнього світу. У статті визначено кіберсуверенітет як індивідуальне самовираження держави в кіберпросторі, що є природною частиною державного суверенітету та визначає технологічну самостійність, інформаційну стійкість і рівень кіберуправління в інформаційному середовищі, гарантуючись відповідною системою зовнішнього, внутрішньонаціонального, адміністративно-правового захисту відповідних об'єктів кіберпростору, на які поширюється юрисдикція держави.

Ключові слова: *адміністративний захист, адміністративні засоби, адміністративно-правові засади, державна інформаційна політика, інформаційна безпека, інформація, кіберпростір, суверенітет.*

Zubko O. M. Cyber sovereignty as a new category in administrative law

Abstract. The relevance of the article is that in today's globalized world, information and databases are the unique resources without the use and preservation of which it is impossible to exist and develop a modern state as a socio-political entity and perform purely military tasks to preserve independence and protection countries. According to experts and analysts of the world's leading countries, the hybridity of modern armed conflict is determined by the presence of a powerful information and cyber component. The purpose of the article is to reveal cyber sovereignty as a new category in administrative law on the basis of a systematic analysis of the positions of scientists, reference materials and norms of current legislation. It is emphasized that with its development, the Internet has gradually become a vital infrastructure for all countries. Recently, cybersecurity issues have been raised in various countries, and countries around the world have begun to create their own cybersecurity systems. Cyber sovereignty is a natural extension of national sovereignty. To meet these challenges, we need to explore the future of cybersecurity for developing countries. It has been found that with its development, the Internet has gradually become a vital infrastructure for all countries of the world. Recently, cybersecurity issues have been raised in various countries, and countries around the world have begun to create their own cybersecurity systems. Cyber sovereignty is a natural extension of national sovereignty. To meet these challenges, we need to explore the future of cybersecurity for developing countries. No state is capable of achieving absolute security. Emphasized respect for cyber sovereignty does not mean disconnecting the Internet and isolating the country from the outside world. The article defines cyber sovereignty as an individual self-expression of the state in cyberspace, which is a natural part of state sovereignty and determines technological independence, information stability and level of cyber governance in the information environment, guaranteed by an appropriate system of external, domestic, administrative and legal protection. cyberspace to which the jurisdiction of the state extends.

Key words: *administrative protection, administrative means, administrative and legal principles, state information policy, informational security, information, cyberspace, sovereignty.*

Актуальність теми. У сьогоднішньому глобалізованому світі інформація й бази даних є тими унікальними ресурсами, без використання та збереження яких неможливе як існування й розвиток сучасної держави як суспільно-політичного утворення, так і виконання суто військових завдань щодо збереження незалежності та захисту країни. На думку експертних кіл та аналітиків провідних країн світу, гібридність сучасного збройного конфлікту визначається саме наявністю потужної інформаційної та кібернетичної складової. Доступ до інформації та захист процесів управління стають визначальними факторами досягнення політичних цілей і військової перемоги [5, с. 85–92].

Нові руйнівні практики розвиваються в кіберпросторі, включаючи злочинне використання Інтернету (кіберзлочинність), шпигунство з політичними або економічними цілями, а також напади на критичну інфраструктуру (транспорт, енергетика, зв'язок тощо) з метою саботажну. З Огляду на урядових чи неурядових гравців, ці кібернапади не обмежуються кордонами або відстанню; є анонімними, дуже важко дійсно визначити справжнього винуватця, який часто діє під прикриттям бот-мереж або посередників; можуть здійснюватися з відносною легкістю, з невеликими витратами або ризиком для зловмисника. Вони мають на меті поставити під загрозу безперебійне функціонування інформаційних і комунікаційних систем, що використовуються громадянами, підприємствами й адміністраціями, і навіть фізичну цілісність інфраструктури, що має вирішальне значення для національної безпеки. Кібербезпека охоплює всі заходи безпеки, які можуть бути вжиті для захисту від цих нападів. Значне зростання складності й інтенсивності кібератак в останні роки змусило більшість розвинених країн посилити свій захист і прийняти національні стратегії кібербезпеки [5, с. 85–92].

Новою категорією у сфері інформаційного середовища та кібербезпеки є кіберсуверенітет, що неоднозначно розуміється науковою спільнотою, однак постійно набуває нових характеристик.

Огляд останніх досліджень. Актуальні питання кіберсуверенітету в контексті адміністративного права в Україні досліджували в наукових доробках такі вчені, як В. Гапотій, О. Герасимова, С. Горова, В. Горовий, С. Демченко, О. Довгань, Д. Дубов, Г. Дугінець, В. Марков, В. Набруско, О. Олійник, А. Письменицький, В. Полевий, О. Радутний, П. Рогов, О. Скрипнюк, О. Солодка, В. Супрун, В. Торяник, А. Череп та інші.

Однак, ураховуючи тривалість гібридної війни, активізацію кібератак державних порталів та інші інформаційні посягання в публічному секторі, актуальність наукових пошуків у сфері кіберсуверенітету набирає нових рис і характеристик.

Мета статті полягає в тому, щоб на основі системного аналізу позицій учених, довідникових матеріалів і норм чинного законодавства розкрити кіберсуверенітет як нову категорію в адміністративному праві.

Виклад основних положень. Актуальність питання про формування нового різновиду правової категорії та предмета правового регулювання як критичної інфраструктури зумовлена тим, що у вітчизняній юриспруденції до цього часу означений різновид предмета правового регулювання й особливо в контексті кібербезпеки та інформаційного суверенітету не розглядався вченими в системі теорії стратегії національної безпеки як самостійний [2, с. 108–109].

Проблема кіберзахисту критичної інфраструктури досить нова для юриспруденції. І хоча за багатовікову історію правової науки дослідженню різноманітних аспектів суверенітету й національної, державної безпеки присвячено безліч праць правознавців різних часів і народів, інформаційна безпека та її складник – кіберзахист критичної інфраструктури – довгий час залишалися за межами фундаментальної юриспруденції. Проте й нині ця проблема є однією з недостатньо розкритих для правознавства, як загальнотеоретичного, так і галузевого. Її актуальність із плином часу не зменшується, а навіть набуває ще більшої гостроти [2, с. 108–109; 5].

Нині в літературі зустрічається концепція, відповідно до якої суверенітету в кіберпросторі немає. Дослідниками відзначається суперечність між принципом суверенітету й самим «духом» інтернету, що ґрунтується на ідеї необмеженого доступу, тоді як державна машинерія надто громіздка, географічно та технологічно

обмежена для регулювання кіберпростору [7, с. 179; 10, с. 830]. Друга лінія аргументації цієї позиції ґрунтується на твердженні, що кіберпростір є загальним надбанням людства (res communis omnium) за аналогією з відкритим морем, міжнародним повітряним простором, відкритим космосом, а тому не підлягає присвоєнню якоюсь державою [11, с. 1645]. Разом із тим більш обґрунтованим, ніж вищевказаний, є інший підхід, згідно з яким державний суверенітет усе ж таки поширюється на кіберпростір. Логічно твердження, що воно per se має на увазі існування відповідної фізичної кіберінфраструктури, яка розташовується на державній території, щодо якої, безперечно, поширюється державна юрисдикція. Крім того, держави мають юрисдикцію щодо заходів, що здійснюються на його території, у кіберпросторі, а також ведуть боротьбу з кіберзлочинами тощо [3, с. 39–44; 9].

Крім того, кіберпростір не може перебувати поза суверенітетом, оскільки державна присутність у кіберпросторі, як демонструють численні інциденти, безпосередньо впливає на її національну безпеку, адже зараз багато держав контролюють деякі елементи своєї критичної інфраструктури (банківська й фінансова системи, транспорт, нафтові й газові магістралі, електропостачання тощо) за допомогою кіберпростору, що водночас робить їх дуже вразливими. Таке твердження підкреслюється в Національній стратегії безпеки кіберпростору США: «У мирний час вороги Америки можуть <…> готуватися до кібератаки, ідентифікуючи інформаційні системи США, визначаючи доступ до основних цілей. У воєнний час супротивники можуть <…> атакувати об'єкти критичної інфраструктури <…> або підривати громадський спокій в інформаційних системах» [12]. Оскільки ймовірність заподіяння шкоди в кіберпросторі реальна, держави не можуть залишити його без управління, а повинні знайти шлях для здійснення контролю в кіберпросторі, щоб зменшити в ньому свою вразливість. Відповідно, як «реальний» світ вимагає державного суверенітету, щоб упорядковувати, захищати й карати різних суб'єктів, так і кіберпростір вимагає такого суверенного впливу [4, с. 3–10].

Як переконаний І. Камінський, держави не можуть здійснювати суверенітет над кіберпростором як віртуальним середовищем, тому що він як об'єкт внутрішньодержавного й міжнародно-правового регулювання є юридичною фікцією, «місцем», яке не існує в об'єктивному світі. Водночас держави володіють суверенними правами щодо об'єктів своєї кіберінфраструктури, а також обов'язками контролювати цю інфраструктуру та запобігати випадкам її умисного використання з метою завдати шкоди іншим державам. Інакше кажучи, формально концепція державного суверенітету поширюється тільки на фізичну територію держави, проте може виходити за межі поняття територіального контролю. Так, Р. Бакен зазначає: «Державний суверенітет захищає від зовнішніх втручань право держави здійснювати певну політику та приймати рішення щодо внутрішніх і зовнішніх питань» [8, с. 223]. Очевидно, що такі питання можуть стосуватися кіберпростору та бути пов'язаними з ним, тому не варто заперечувати зв'язок державного суверенітету з кіберпростором [4, с. 3–10].

А. Жалдибін говорить про дихотомічний характер аналізованої проблематики: з одного боку, здійснення кібератак негативно впливає на систему міжнародної безпеки, унаслідок чого закономірною є робота щодо запобігання їм у тому числі за допомогою встановлення правил поведінки в кіберпросторі; проте, з іншого боку, саме правове регулювання може розвинутися лише базуючись на субстантивній державній практиці, а в цьому випадку – практиці здійснення кібератак однією державою щодо іншої, що спричинило серйозні наслідки. Наприклад, якщо у відповідь на кібератаку на об'єкт критичної інфраструктури (атомну електростанцію тощо) держава відповість кінетичною атакою в порядку реалізації права на самооборону. Ця ситуація стане тим необхідним потужним імпульсом розвитку правового регулювання кібербезпеки, який сприятиме пошуку відповіді на наявні питання. Одного інциденту буде недостатньо для розвитку регулювання, як, наприклад, у випадку із запуском першого штучного супутника Землі-4 жовтня 1957 року в контексті космічного права. Доступ до космічного простору через технологічні, фінансові та інші аспекти фактично має лише неве-

лику кількість держав, а формування практики в цій галузі пов'язане з великим витрачанням ресурсів. У свою чергу, кіберпростір покриває абсолютно всі без винятку країни незалежно від рівня їхнього розвитку. Очевидно, що здійснення руйнівних кібератак ipso facto передбачає наявність розвиненої технологічної бази, проте доступ до цього середовища не передбачає значних обмежень. Це дає підстави вважати, що досить велике коло суб'єктів теоретично зможе зробити внесок у розвиток необхідної практики, більший, ніж коло держав, що форсують формування практики за іншими сферами міжнародного права [3, с. 39–44].

У міру свого розвитку Інтернет поступово став життєво необхідною інфраструктурою для всіх країн світу. Останнім часом у різних країнах виникають питання, пов'язані з кібербезпекою, і держави всього світу почали створювати власні системи кібербезпеки. Кіберсуверенітет є природним продовженням національного суверенітету. Для відповіді на ці виклики необхідно вивчити майбутнє кібербезпеки для країн, що розвиваються. Жодна держава не здатна домогтися абсолютної безпеки. Підкреслена повага до кіберсуверенітету не означає відключення Інтернету й ізоляції країни від зовнішнього світу. Міжнародне співтовариство має створити новий порядок кіберуправління, заснований на взаємній повазі кіберсуверенітету та суверенної рівності. Майбутнім кіберсуверенітетом має стати спільне управління [1].

Кібератаки бувають найрізноманітніших форм і можуть перемогти навіть найкращі заходи кібербезпеки. У сучасному середовищі кіберзагроз без кордонів нації по всьому світу постійно намагаються зберегти ініціативу над своїми кіберворогами. У рамках цього процесу вони повинні оцінити свій кіберсуверенітет, щоб знати, наскільки добре вони контролюють безпеку кіберпростору, який використовується на їхній території та для своєї діяльності за кордоном. Кіберсуверенітет нації залежить від багатьох факторів, таких як технологічна залежність від іноземних країн та існування національних можливостей кіберстійкості. Але політичні міркування, рівень зрілості зацікавлених сторін, складність екосистеми кіберуправління й інші ключові критерії також впливають на те, наскільки швидко та наскільки кіберсуверенітет варто й можна покращити [6].

Узагальнюючи, можна підкреслити, що кіберсуверенітет є новою категорією в адміністративному праві України, що сформоване в результаті розвитку кіберпростору та створене для захисту інтересів держави як суб'єкта інформаційного середовища.

Отже, кіберсуверенітет – це індивідуальне самовираження держави в кіберпросторі, що є природною частиною державного суверенітету й визначає технологічну самостійність, інформаційну стійкість і рівень кіберуправління в інформаційному середовищі, гарантуючись відповідною системою зовнішнього, внутрішньонаціонального, адміністративно-правового захисту відповідних об'єктів кіберпростору, на які поширюється юрисдикція держави.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Вэньхун Сюй. Вызовы кибер-суверенитету и ответные меры. *Мировая экономика и международные отношения.* Том 64. Вып. № 2. С. 89–99.

2. Гапотій В.Д. Кібернетичний суверенітет держави: правовий підхід. *Актуальні проблеми інформаційного права в умовах глобалізації :* збірник тез доповідей учасників Всеукр. наук.-практ. інтернет-конф. Київ, 2019. С. 108–109.

3. Жалдыбин А.В. Международные отношения: история, теория, практика. *Материалы IX науч.-практ. конф. молодых ученых фак. междунар. отношений БГУ*. Минск : БГУ, 2019. С. 39–44.

4. Камінський І.І. Концепція державного суверенітету в контексті застосування кіберсили. *Альманах міжнародного права.* 2017. Вип. 16. С. 3–10.

5. Мальцева І.Р. Кібербезпека – одна з найважливіших складових всієї системи захисту у збройних силах України. *Кібербезпека: освіта, наука, техніка.* 2020. № 1. С. 85–92.

6. A nation's journey towards Cyber Sovereignty. Thales Group. URL: https://www.thalesgroup.com/en/markets/defence-and-security/cyberdefence-solutions/cyber-sovereignty.

7. Boyle J. Foucault in cyberspace: surveillance, sovereignty and hardwired censors. *University of Cincinnati law review.* 1997. Vol. 66. P. 177–206.

8. Buchan R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law.* 2012. Vol. 17. № 2. P. 211–227.

9. Cyberspace Policy Report to Congress Pursuant to the National Authorization Act for fiscal year 2011. URL: https://nsar-chive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.

10. Lotrionte C. State sovereignty and self-defense in cyberspace: a normative framework for balancing legal rights. *Emory international law review.* 2012. Vol. 26. P. 825–919.

11. Shmitt N., Vihul L. Respect for Sovereignty in Cyberspace. *Texas law review.* 2017. Vol. 95. P. 1640–1671.

12. The National Strategy to Secure Cyberspace (February 2003). URL: https://www.us-cert.gov/sites/default/files/publications/ cyberspace_strategy.pdf.