

УДК: 327.8:342.9:004.9

DOI: 10.60022/2(4)-5S

Білоусов Олександр Сергійович

доктор політичних наук, професор кафедри міжнародних відносин та права
Національний університет «Одеська політехніка», Україна

Bilousov Oleksandr

Doctor of Political Sciences, Professor of the Department of International Relations and Law
National University «Odesa Polytechnic», Ukraine
ORCID: 0009-0009-2533-7287

Кривдіна Інна Борисівна

кандидат історичних наук, доцент кафедри
міжнародних відносин та права
Національний університет «Одеська політехніка», Україна

Kryvdina Inna

Candidate of Historical Sciences, Associate Professor of the Department
of International Relations and Law
National University «Odesa Polytechnic», Ukraine
ORCID: 0000-0002-1472-3037

ЗОВНІШНЯ ПОЛІТИКА ДЕРЖАВ АТР В КОНТЕКСТІ ГЕОПОЛІТИКИ ІНФОРМАЦІЙНОГО ВПЛИВУ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Анотація. У статті здійснено аналітичне дослідження трансформації зовнішньої політики держав Азійсько-Тихоокеанського регіону (АТР) під впливом геополітики інформаційного впливу та цифрових технологій. Розглянуто, як цифрова трансформація, кіберінфраструктура та нові інформаційні стратегії змінюють зовнішньополітичні підходи таких країн, як Китай, США, Австралія та інших учасників КВАД. Акцент зроблено на інформаційній конкуренції, побудові цифрового суверенітету, боротьбі за контроль над глобальними інформаційними потоками та підводними телекомунікаційними кабелями. Виявлено, що держави АТР активно використовують інформаційний вплив як інструмент м'якої сили та геостратегічного тиску, застосовуючи інструменти дезінформації, цифрової дипломатії, контроль за даними та інфраструктурою. На основі аналізу кейсів сформульовано висновки щодо посилення інформаційної складової в зовнішній політиці та потреби в нових формах міждержавної цифрової співпраці. Запропоновано модель «інформаційного меркантилізму» як аналітичну рамку для опису сучасної зовнішньополітичної поведінки в умовах цифрової геополітики. Результати дослідження можуть бути використані для формування стратегій цифрової дипломатії, протидії інформаційним загрозам і посилення міжнародної кіберспівпраці.

Ключові слова: геополітика, інформаційний вплив, зовнішня політика, цифрова трансформація, АТР, КВАД, інформаційний суверенітет, кіберінфраструктура, кібердипломатія.

FOREIGN POLICY OF APAC STATES IN THE CONTEXT OF THE GEOPOLITICS OF INFORMATION INFLUENCE AND DIGITAL TRANSFORMATION

Abstract. This article provides an analytical study of how the foreign policies of Asia-Pacific countries (APAC) are transforming under the influence of information geopolitics and digital technologies. It explores the impact of digital transformation, cyberinfrastructure, and new information strategies on the foreign policy approaches of China, the United States, Australia, and other QUAD members. The study emphasizes the growing importance of information competition, digital sovereignty, control over global data flows, and submarine cable infrastructure. It reveals that APAC states increasingly employ informational influence as a tool of soft power and geopolitical pressure, utilizing disinformation, digital diplomacy, data localization policies, and infrastructure control. Based on selected case studies, the paper concludes that information has become a core element in contemporary foreign policy and underlines the necessity for new formats of intergovernmental digital coordination. The concept of “informational mercantilism” is proposed as an analytical framework to describe state behavior in the era of digital geopolitics. The findings can inform strategies in digital diplomacy,

countering informational threats, and enhancing international cyber cooperation.

Keywords: *geopolitics, informational influence, foreign policy, digital transformation, Asia-Pacific, QUAD, information sovereignty, cyber infrastructure.*

Постановка проблеми. Сучасна епоха цифрових трансформацій спричинила радикальні зміни у сфері міжнародних відносин, зовнішньої політики та геополітичного суперництва. У сучасній науці поняття «геополітика інформаційного впливу» формується на перетині теорій міжнародних відносин, інформаційної безпеки, цифрової дипломатії та критичної геополітики. Особливо це відчутно у регіоні Азійсько-Тихоокеанського регіону (АТР), який є одним із найдинамічніших центрів глобальної сили. Зовнішня політика держав у цьому регіоні дедалі більше формулюється та реалізується крізь призму інформаційного впливу, контролю над цифровою інфраструктурою, кібербезпеки та стратегічного управління даними. Геополітика поступово виходить за межі територіального домену, охоплюючи нову площину інформаційний простір, де держави змагаються не лише за території чи ре-сурси, а й за увагу, довіру, сприйняття та вплив, цифрові технології змінюють способи ведення зовнішньої політики й міжнародної інформаційної взаємодії.

У цьому контексті інформаційний вплив стає не тільки інструментом «м'якої сили», а й важелем конкурентної боротьби, підпорядкованим загальній зовнішньополітичній стратегії. Китай, США, Японія, Австралія, Південна Корея, Індія та інші країни АТР реалізують власні цифрові ініціативи, створюють регіональні альянси, впроваджують законодавчі механізми цифрового суверенітету та розвивають нові формати дипломатії – від кібердипломатії до цифрової кооперації в межах QUAD, IPEF, ASEAN Digital Masterplan тощо.

Трансформація зовнішньої політики під впливом інформаційних і цифрових факторів є однією з найменш досліджених тем у вітчизняній і частково зарубіжній політології та міжнародних дослідженнях. Попри зростаючу кількість робіт, присвячених інформаційній безпеці, дезінформації, кіберзагрозам, все ще бракує системного аналізу того, як інформаційні стратегії впливають на зовнішньополітичну поведінку держав, зокрема в регіоні АТР.

Наразі потребує наукового осмислення низка пов'язаних питань:

Яку роль відіграє інформаційний вплив у формуванні зовнішньої політики держав АТР? Як цифрова трансформація змінює формат, зміст і канали міжнародного впливу? Які механізми інформаційного контролю застосовують держави для посилення своєї геополітичної позиції?

Відповіді на ці питання дозволять не тільки глибше зрозуміти логіку зовнішньополітичного вибору, а й сформулювати засади для формування національних цифрових стратегій.

Дослідження спирається на міждисциплінарний теоретичний фундамент, що поєднує концепції геополітики, інформаційної безпеки, цифрової дипломатії та теорії міжнародних відносин.

Аналіз останніх досліджень і публікацій. Упродовж останнього десятиліття проблематика цифрової трансформації у сфері міжнародних відносин і зовнішньої політики привертає все більше уваги з боку зарубіжних і вітчизняних дослідників. Зростаюче розуміння ролі інформаційних технологій як стратегічного ресурсу зумовило появу широкого спектру досліджень, у яких аналізуються аспекти інформаційного впливу, кібербезпеки, цифрового суверенітету та їхнє місце у сучасній геополітиці.

Проблематика геополітики інформаційного впливу дедалі частіше стає предметом міждисциплінарного дослідження.

Серед провідних зарубіжних дослідників, які зробили суттєвий внесок у розробку теоретичних основ інформаційної геополітики, слід відзначити: Дж. Най (Joseph S. Nye) [6; 17; 18] – автор концепції «м'якої сили» та «розумної сили», що акцентує увагу на немілітаризованих формах впливу, у тому числі інформаційних. У праці «The Future of Power» (2011) [17] він розглядає інформацію як стратегічний ресурс XXI століття, також увів поняття «smart power» та «cyber power» у міжнародні відносини; П. Ван Гем (Paul van Ham), який акцентував на «брендуванні» держави в глобальному інформаційному просторі; М. Клімбург (M. Klimburg), котрий розробив концепцію «інформаційного конфлікту» та «цифрової автономії»; David Shambaugh та Evan Feigenbaum – аналізують трансформацію зовнішньої політики Китаю в умовах цифрової доби та її глобальний проєкційний вплив через ініціативи на кшталт «Цифрового Шовкового шляху»; Samantha Hoffman [16] та Elsa Kania – висвітлюють концепт «технологічного авторитаризму» у китайській зовнішній політиці, зокрема в дослідженнях Австралійського інституту стратегічної політики (ASPI); Richard Fontaine та Kiron Skinner – досліджують конкурентність цифрових стратегій США та створення альянсів типу QUAD для протидії впливу КНР.

У контексті АТР дослідження проводили С. Мерц (S. Mertz), Р. Грей (R. Gray), В. Цзюнь (Weijian Zhu) та інші, аналізуючи вплив Китаю та США на цифрову політику регіону. Водночас комплексного аналізу інформаційної геополітики держав АТР з урахуванням новітніх цифрових ініціатив, таких як QUAD Digital Cooperation [19] та ASEAN Digital Masterplan [9], у науковій літературі ще бракує.

В українському науковому дискурсі проблематика інформаційної геополітики в контексті АТР досліджується фрагментарно. Водночас у працях таких авторів, як: О. І. Толмачова («Цифрова дипломатія як новий інструмент зовнішньої політики держав», 2021) акцентується увага на трансформації традиційних дипломатичних інструментів під впливом цифрових технологій; О. Ю. Литвиненко («Інформаційна безпека в міжнародних відносинах: нові виклики», 2020) аналізує роль інформаційної безпеки в контексті зовнішньої політики та національної безпеки; І. В. Кабаненко («Цифрова стратегія і глобальна безпека», 2022) розглядає цифрову трансформацію як фактор нової глобальної конкуренції; Ю. Казмірчук («Інформаційна політика країн Азійсько-Тихоокеанського регіону», 2023) – дає регіональний зріз інформаційних ініціатив у країнах АТР.

Також варто згадати аналітичні доповіді від Belfer Center for Science and International Affairs (Harvard University), Brookings Institution, Center for Strategic and International Studies (CSIS), Digital Asia Hub, де оприлюднено системні огляди цифрової зовнішньої політики США, Китаю, Японії та Австралії.

Попри значну кількість публікацій, варто зазначити, що саме системне поєднання інформаційного впливу, зовнішньої політики та регіональної специфіки АТР у єдину аналітичну рамку залишається недостатньо опрацьованим. Більшість наявних досліджень фокусуються на окремих елементах – дезінформації, кібербезпеці або цифровій дипломатії – без глибокого узагальнення та порівняльного аналізу між державами.

Отже, в статті зосередимось на комплексному вивченні інформаційного компоненту зовнішньої політики держав АТР в умовах цифрової трансформації.

Метою статті є дослідити геополітику інформаційного впливу в зовнішній політиці держав АТР через призму регіональної цифрової інтеграції, технологічного суперництва та кібердипломатії, оцінити, як цифрова трансформація та інформаційний вплив формують зовнішню політику держав АТР.

Завдання дослідження:

- охарактеризувати поняття «геополітика інформаційного впливу» в сучасному міжнародному дискурсі, описати геополітичний інформаційний ландшафт;
- проаналізувати зовнішньополітичні стратегії ключових акторів АТР у сфері цифрової політики;
- порівняти підходи QUAD і ASEAN до формування цифрового суверенітету та кібербезпеки;
- оцінити вплив цифрової інфраструктури (підводні кабелі, кібербезпека);
- розкрити роль інформаційної резиліентності та кібердипломатії в регіональній стабільності.

Виклад основного матеріалу. У першій чверті XXI століття цифровий розвиток країн Азіатсько-Тихоокеанського регіону набуває геостратегічного значення. Регулювання цифрового простору перетворюється на арену протистояння інформаційних моделей – демократичної (QUAD, ЄС, Японія) та авторитарної (Китай, у меншій мірі – Росія).

Країни QUAD [19], передусім США, Австралія, Японія та Індія, розвивають ініціативи зі створення цифрового альянсу, орієнтованого на: прозоре управління даними, обмеження експансії компаній, пов'язаних із авторитарними режимами, підтримку цифрових прав і свобод. Ці країни, зокрема Японія й Австралія, активно інвестують у кіберрезиліентність країн Південно-Східної Азії, утверджуючи нові стандарти інформаційного суверенітету.

Натомість держави ASEAN [9] намагаються маневрувати між цифровими гравцями, зберігаючи інформаційну рівновагу та прагматичний баланс. Їхній підхід полягає у: розбудові національної цифрової інфраструктури, захисті інформаційних кордонів, розвитку внутрішнього ринку електронних послуг, посиленні регіональної взаємодії без радикального геополітичного вибору.

ASEAN Digital Masterplan 2025 демонструє зростаюче усвідомлення важливості цифрового суверенітету, проте у гнучкому, інклюзивному форматі, який уникає жорсткої блокової конфронтації.

Таким чином, цифрові стратегії в АТР відображають геополітичну поляризацію регіону, де QUAD представляє проактивну модель інформаційної сили, тоді як ASEAN обирає модель обережного балансування в умовах технологічного суперництва. Обидва підходи формують нову цифрову архітектуру регіону, яка суттєво впливатиме на світовий порядок у наступні десятиліття.

Взагалі, ідеї про вплив без застосування прямої сили були закладені в концепції «м'якої сили»

(soft power), яку сформулював Дж. Най (Joseph Nye) [6]. Згідно з нею, держави можуть досягати своїх зовнішньополітичних цілей, апелюючи до цінностей, культури, переконань і легітимності дій, а не лише військовими або економічними засобами (Nye, 2004) [18]. В цифрову епоху м'яка сила все більше спирається на інформаційні технології як механізм комунікації та проєкції впливу. У продовження цієї думки, Мануель Кастельс розвинув уявлення про «мережеву владу» (network power), у якій ключовим ресурсом стає інформація, а контроль за нею – новою формою домінування у світовій політиці (Castells, 2010) [10].

Геополітичний вимір інформаційного впливу спирається на уявлення про інформацію не лише як знання, а як інструмент впливу через формування наративів та образу «іншого», маніпуляцію громадською думкою, вплив на політичні рішення через дезінформацію або приховану агітацію, контроль за інформаційною інфраструктурою (мережі, хмари, платформи, кабелі тощо). У цьому контексті інформаційна влада (information power) постає як можливість однієї держави впливати на інформаційне середовище іншої держави або групи держав, нав'язуючи їм вигідні смислові конструкти (Walker, 2016) [21].

Поняття «цифрової геополітики» виникає у відповідь на зростання ролі ІТ у глобальній конкуренції. На думку Лінча та Шапіро (Lynch & Shapiro, 2021), цифрові платформи стали новим простором зіткнення державних інтересів, у якому ведеться боротьба не лише за технологічну перевагу, але й за нормативний контроль над даними, алгоритмами, потоками контенту. В цьому аспекті особливе значення мають:

- «цифровий суверенітет» (digital sovereignty) - прагнення держав контролювати власний інформаційний простір та цифрову інфраструктуру в межах національної юрисдикції;
- «кіберсуверенітет» (cyber sovereignty) – концепт, активно просуваний Китаєм;
- «інформаційна асиметрія» яка створює залежність менш розвинених держав від інформаційних потоків із глобальних центрів сили.
- «кібердипломатія» – сукупність дипломатичних інструментів, політик і переговорних практик у сфері регулювання кіберпростору, цифрової безпеки та транснаціонального обміну даними;
- «інформаційна резилієнтність» – здатність суспільства або держави протистояти зовнішньому інформаційному впливу, фейкам, пропаганді, зберігаючи критичне мислення, інформаційну цілісність і стратегічну стабільність;
- «інформаційний меркантилізм» – теоретична модель, яка описує державну стратегію накопичення інформаційних ресурсів, контролю над обміном даними та використання їх як економічного й політичного капіталу.

На основі вищезазначених теорій можна визначити геополітику інформаційного впливу як сукупність цілеспрямованих дій держави (або коаліції держав), що мають на меті забезпечення домінування або зміцнення позицій у міжнародному середовищі через контроль, модифікацію чи монополізацію інформаційних потоків, технологій передачі даних та інфраструктур цифрової комунікації. Це форма використання інформаційних ресурсів для досягнення зовнішньополітичних цілей. Така форма впливу поєднує традиційні методи дипломатії з сучасними інструментами – соціальними мережами, медіа-кампаніями, маніпулюванням цифровими платформами що включає створення і поширення стратегічних наративів (Narrative Power), дипломатичне просування стандартів і норм у сфері ІКТ (Digital Diplomacy), участь у глобальних альянсах на кшталт QUAD, AUKUS, ASEAN Digital Masterplan; використання інформаційної присутності для м'якого впливу або прихованого тиску.

У відповідь на виклики цифрової доби, держави Азіатсько-Тихоокеанського регіону активізували регіональні формати співпраці у сфері інформаційної безпеки, цифрової трансформації та формування спільного геополітичного порядку денного. Серед них особливе значення мають Індो-Тихоокеанське партнерство QUAD та Цифровий план розвитку ACEAN (ASEAN Digital Masterplan 2025) [9].

QUAD (Quadrilateral Security Dialogue – технологічна коаліція стратегічного балансу) [19] – це стратегічний діалог між Австралією, Індією, Японією та США, який поступово еволюціонував із безпекового формату до широкої платформи співпраці, зокрема в цифровій, інформаційній та технологічній сферах. В умовах зростання впливу Китаю, QUAD дедалі більше позиціонується як аналітична та проактивна відповідь на цифрову геополітику регіону.

У рамках співпраці у сфері технологій та інформаційної безпеки, QUAD визначає такі пріоритети:

- розвиток безпечних ланцюгів постачання ІТ-обладнання (зокрема 5G/6G технологій);
- координація стандартів з кібербезпеки та штучного інтелекту;
- протидія дезінформації та зміцнення демократичної резилієнтності інформаційного простору

(QUAD, 2022) [19].

У 2021 році держави QUAD створили Спільну робочу групу з критичних та новітніх технологій (Critical and Emerging Technology Working Group), яка координує політику в сфері AI, Big data, квантових технологій, кіберзахисту та цифрової інфраструктури (White House, 2021). Країни QUAD активно просувають технології, що забезпечують цифрову автономію, такі як 5G, блокчейн, штучний інтелект. Підхід акцентує увагу на важливості технологічних стандартів та відкритих Інтернет-просторів.

Таким чином, QUAD формує альтернативну інформаційну геостратегію, в якій цифрова суверенність, прозорість, етичні норми поведінки з даними та відкритість ІТ-інфраструктури виступають засобом протидії авторитарним цифровим моделям.

Усвідомлюючи необхідність синхронізації цифрової трансформації та збереження інформаційного суверенітету, Асоціація держав Південно-Східної Азії (ASEAN) у 2021 році ухвалила Цифровий майстер-план розвитку на 2021–2025 роки (ASEAN Digital Masterplan 2025, або ADM2025 [9]). Оскільки більшість країн ASEAN є розвиваються, акцент робиться на підвищенні кіберрезилієнтності, зокрема через навчання, обмін кращими практиками та створення центрів реагування на кіберінциденти (CERT ASEAN).

ADM2025 визначає стратегічні напрями для створення інтегрованого, захищеного, сталого та інклюзивного цифрового простору в Південно-Східній Азії, зокрема: розвиток інфраструктури широкосмугового доступу, цифровізація державного управління, зміцнення кібербезпеки через спільні стандарти, запобігання кіберзагрозам і фейковим новинам, підтримка цифрової економіки та інновацій. У межах ADM2025, ASEAN реалізує конкретні ініціативи, зокрема ASEAN Cybersecurity Cooperation Strategy, Digital Data Governance Framework, а також сприяє створенню єдиного ринку цифрових послуг у регіоні (ASEAN Secretariat, 2021) [9]. Важливо, що ADM2025 формує інформаційно-технологічну ідентичність регіону, зберігаючи баланс між кооперацією з глобальними акторами (США, ЄС, Китай) і захистом власних інформаційних пріоритетів. Це – спроба відстояти інформаційний нейтралітет, уникаючи жорсткої поляризації між технологічними блоками.

Отже, ініціативи QUAD і ADM2025 є прикладами того, як інформаційна складова зовнішньої політики держав АТР інтегрується у стратегії регіонального розвитку. У фокусі не лише розвиток технологій, а й контроль над смислами, цифровими потоками, інформаційними стандартами, що підтверджує активізацію геополітики інформаційного впливу в регіоні.

АТР сьогодні перебуває у фокусі численних гібридних загроз, що охоплюють кібератаки на інфраструктуру, інформаційні кампанії впливу, маніпуляції в соціальних мережах, а також втручання у виборчі процеси через цифрові платформи. Особливо вразливими є країни з недостатньо розвиненими інституціями кібербезпеки — наприклад, М'янма, Камбоджа чи Лаос. Водночас навіть високотехнологічні держави, як Японія чи Південна Корея, стикаються з проблемами захисту даних, розповсюдження фейкових новин і зовнішніх впливів на цифрову політику.

Дезінформаційні кампанії, які активно використовуються Китаєм і росією для просування власних наративів, підривають довіру до демократичних інституцій і ускладнюють регіональну координацію. Такі кампанії спрямовані не лише на дискредитацію політичних лідерів або альянсів, як-от QUAD, а й на вплив на молодь та освітнє середовище через TikTok, WeChat та інші платформи.

У відповідь на виклики інформаційної безпеки країни АТР дедалі активніше вдаються до кібердипломатії як інструменту зміцнення регіональної стабільності. Кібердипломатія передбачає взаємне визнання цифрових стандартів, укладення угод щодо захисту критичної інфраструктури, спільні тренування CERT-груп та обмін інформацією між національними центрами кібербезпеки.

Як вже зазначалося вище, QUAD (США, Індія, Австралія, Японія) просуває ідею «вільного та відкритого кіберпростору», де держави координують політику щодо кіберзагроз, критичної інфраструктури й дезінформації. В межах Quad Cybersecurity Partnership розроблено рамкові механізми обміну кіберданими та створено кібераналізаторську групу; ASEAN, у свою чергу, в межах Digital Masterplan 2025 запроваджує механізми кіберрезилієнтності шляхом гармонізації цифрових стандартів, створення CERT ASEAN, інвестування в цифрову освіту та реагування на інформаційні загрози.

Кібердипломатія в регіоні має не лише оборонний, а й конструктивний вимір - вона сприяє налагодженню міждержавної довіри, спільному протистоянню загрозам цифрової епохи та формуванню нового порядку в інформаційному просторі АТР. Так, інформаційний вплив стає визначальним інструментом невоєнного, проте стратегічного впливу на міжнародному рівні. У країнах АТР, особливо в Китаї, США, Японії, Південній Кореї та Австралії, інформаційні стратегії розглядаються як елемент державного управління і дипломатії. Йдеться про:

- формування іміджу держави у глобальних медіа, вплив на міжнародну громадську думку (public diplomacy);
- інформаційне моделювання наративів – держави просувають свої версії історії, безпеки, торгівлі тощо (наприклад, «цифровий Шовковий шлях» Китаю або «вільний і відкритий Індो-Тихоокеанський регіон» США та Японії);
- застосування інформаційної «м'якої сили» для досягнення політичних цілей без прямого втручання - через культурні, освітні, технічні й інфраструктурні програми (наприклад, хмарні обчислення, цифрові гранти, інвестиції у підводні кабелі тощо);
- проведення інформаційних операцій у кіберпросторі та соціальних медіа – з метою дестабілізації або просування власних інтересів (Китай і росія демонструють такі підходи щодо Тайваню, Південно-Східної Азії тощо).

Інформаційний вплив у ХХІ столітті є дешевшим і швидшим, ніж військовий тиск, однак часто - не менш ефективним.

Що стосується цифрової трансформації, то вона призвела до докорінної зміни засобів і логіки зовнішньополітичного впливу:

- з'явилися нові канали впливу – соціальні мережі, цифрові платформи (TikTok, WeChat, X/Twitter, YouTube), які стали не лише комунікаційними середовищами, а й аренами геополітичного суперництва;
- змінився формат дипломатії – дипломатичні меседжі, політичні заяви й навіть міжнародні конфлікти дедалі частіше мають цифрову форму реалізації (кібердемарші, онлайн-самміти, дипломатичні кампанії в соцмережах);
- поява цифрових технологій як засобу проєкції сили – штучний інтелект, великі дані (big data), хмарні сервіси, блокчейн – інструменти нової «цифрової державності», що формують вплив без фізичної присутності;
- формування нових альянсів, таких як IPEF (Indo-Pacific Economic Framework), QUAD Cybersecurity Working Group, ASEAN Digital Masterplan, що об'єднують держави заради спільного реагування на цифрові виклики.

Таким чином, зовнішня політика перестає бути лише ареною міністерств закордонних справ – тепер це багаторівнева взаємодія між державами, платформами, компаніями, технологіями та суспільствами. А АТР є епіцентром боротьби за контроль над інформаційними потоками, інфраструктурою та наративами. Держави застосовують технологічні, нормативно-правові, інституційні, геоінфраструктурні механізми.

До технологічних можна віднести фільтрацію, цензуру та обмеження доступу до певних платформ (наприклад, Великий Фаєрвол у КНР), вимоги зберігати дані користувачів на території держави (Індія, Китай); побудову альтернативної цифрової інфраструктури, як прокладку власних підводних кабелів, запуск національних супутникових мереж, розвиток локальних хмарних платформ.

Прийняття законодавства про кіберсуверенітет (наприклад, «Cybersecurity Law of China», «Digital Security Act» в Індонезії), угоди про обмін даними (Data Free Flow with Trust - Японія, стандарти CBPR - США, Південна Корея, Тайвань); національні стратегії цифрової дипломатії - як, наприклад, у Сінгапурі чи Австралії – основні нормативно-правові напрямки. Прикладами інституційних механізмів можуть бути Центри інформаційного аналізу та протидії дезінформації (наприклад, Австралійський центр дезінформаційної безпеки), співпраця з Big Tech-компаніями з метою просування державних пріоритетів.

Інвестиції в цифрову інфраструктуру країн регіону як спосіб створення політичної залежності (наприклад, ініціатива «Digital Silk Road» КНР), контроль над підводними телекомунікаційними кабелями (США та Австралія конкурують із Huawei Marine у Південно-Тихоокеанському регіоні) – основні напрямки розвитку геоінфраструктури.

Детальніше розглянемо напрямки політики деяких країн АТР:

КНР розглядає інформаційну сферу як ключовий фронт геополітичного суперництва. Основні характеристики китайської моделі:

- ініціатива «Цифровий Шовковий шлях» – складова ініціативи «Один пояс – один шлях», яка передбачає побудову цифрової інфраструктури в країнах-партнерах (кабелі, 5G, смарт-міста), зокрема в Південно-Східній Азії, Африці, Латинській Америці;
- цифровий суверенітет – концепт, за якого держава повністю контролює Інтернет-простір усередині країни та прагне поширити відповідну модель на міжнародному рівні;
- просування китайських платформ (Huawei, ZTE, Alibaba Cloud) як альтернативи західним гігантам (Amazon, Google, Cisco);

- активна участь у формуванні норм кіберпростору через ООН, BRICS, SCO, де КНР лобіює норми, що легітимізують державний контроль над даними.

Отже, Китай поєднує економічну вигоду з політичним впливом, пропонуючи державам «пакетне рішення»: інфраструктура + кредити + політична підтримка.

США виступають за збереження глобального, вільного, прозорого Інтернету й водночас реалізують жорстку технологічну конкуренцію з КНР. Основними інструментами є: ініціатива «Clean Network» (2020), яка спрямована на виключення китайських компаній зі світових телеком-ланцюгів; створення Індо-Тихоокеанських цифрових альянсів (QUAD, IPEF), що включають компоненти кібербезпеки, обміну даними та спільного інвестування в цифрову інфраструктуру; експорт американських стандартів у сфері конфіденційності, штучного інтелекту, цифрової торгівлі через підтримку ініціатив OECD, WTO, G7; геоекономічний тиск – накладення санкцій на китайські технологічні компанії (Huawei, TikTok), стимулювання повернення виробництва чипів (CHIPS Act, 2022). Взагалі, США розглядають цифрову трансформацію як простір для проєкції ліберальних цінностей, але у поєднанні з реалістичною конкуренцією за контроль над глобальними мережами.

Австралія, як регіональний кібергравець і гарант прозорості виступає стратегічним партнером США в регіоні та водночас є самостійним гравцем у сфері цифрової політики:

- заборона Huawei і ZTE на участь у 5G-інфраструктурі з міркувань національної безпеки (ще у 2018 році – одна з перших країн);

- існує програма підтримки цифрової інфраструктури Тихоокеанських країн – надання фінансування для побудови кабельних ліній (Coral Sea Cable);

- австралійський центр протидії дезінформації – приклад формування стійких інституцій, що поєднують уряд, науку та громадськість;

- регіональні дипломатичні ініціативи (Digital Pacific Partnership, ASEAN-Australia Digital Trade Standards) – спрямовані на просування «прозорої та безпечної» цифрової архітектури.

Австралія прагне бути посередником між техногігантами й державами, які потребують доступу до надійних цифрових рішень, позиціонуючи себе як «чесного брокера» в АТР.

Все це ілюструє, що інформаційний вплив і цифрова трансформація стали не просто допоміжними інструментами зовнішньої політики, а фундаментальними компонентами геополітичного суперництва в АТР. Тому аналіз цих процесів є ключовим для розуміння майбутнього міжнародних відносин у цьому регіоні й показує, що держави АТР водночас і конкурують, і змушені співпрацювати у сфері цифрової безпеки: наприклад, Австралія, Японія та Індія мають спільні ініціативи з кіберстійкості, але одночасно захищають власні цифрові ринки від китайських технологій; США й Китай демонструють асиметричну конкуренцію – де кожна сторона намагається нав'язати світові власну цифрову парадигму.

Таким чином, цифрова зовнішня політика АТР сьогодні базується на парадоксальному поєднанні кооперації (для безпеки) та стратегічної недовіри (для контролю). Саме АТР є головною ареною цифрово-інформаційного геополітичного суперництва, де зовнішня політика трансформується під впливом технологій, кібербезпеки й інформаційного тиску. Китай, США та Австралія демонструють три різні моделі цифрового впливу:

- Китай – централізовано-інфраструктурну модель із пріоритетом контролю;

- США – відкриту модель із наголосом на глобальних стандартах;

- Австралія – регіональну модель з акцентом на прозорість і партнерство.

Геополітика інформаційного впливу в Азіатсько-Тихоокеанському регіоні в умовах цифрових трансформацій вимагає нових підходів до зовнішньої політики та міжнародних відносин. Цифрові технології стали важливим інструментом геополітичної боротьби, що змушує держави розробляти нові стратегії інформаційної безпеки та співпраці в кіберпросторі. Підводні кабелі, BGP-контроль, цифрові платформи – нові об'єкти зовнішньополітичної боротьби, що замінюють традиційні сфери впливу. Виникає небезпека фрагментації цифрового простору, де держави змушені «обирати» між цифровими блоками, що послаблює глобальну інтегрованість. Водночас, з'являються інституційні платформи для співпраці, що можуть забезпечити стабільність у цифровому регіональному порядку.

Висновки. У результаті дослідження було встановлено, що інформаційна резилієнтність є важливим фактором забезпечення стабільності не лише в контексті національної безпеки, а й у межах регіональних союзів. Країни АТР, враховуючи численні виклики дезінформації та цифрових загроз, активно співпрацюють у рамках ініціатив QUAD та ASEAN для підвищення своєї кібербезпеки та забезпечення цифрового суверенітету. Обидва альянси активно просувають цифрові стратегії, націлені на захист критичної інфраструктури, боротьбу з кібератаками та збереження стабільності в

інформаційному просторі.

Одним із ключових аспектів, що забезпечують успіх регіональної стабільності, є кібердипломатія, яка дозволяє країнам АТР спільно протистояти інформаційним загрозам, зміцнювати міждержавну довіру та налагоджувати механізми швидкого реагування на кіберзагрози. Кібердіяльність держав у межах QUAD та ASEAN стає не тільки засобом забезпечення національної безпеки, а й важливим інструментом для досягнення стратегічних цілей у зовнішній політиці.

Також, цифрова трансформація та геополітика інформаційного впливу дедалі більше визначають зміст і механізми зовнішньої політики держав Азійсько-Тихоокеанського регіону. Інформація, дані та інфраструктура їхньої передачі стали новими елементами стратегічної боротьби, порівнюваними за значенням із традиційною військово-економічною конкуренцією. Отже:

1. Геополітика інформаційного впливу – поняття виникло на стику класичної геополітики та інформаційних досліджень (Castells, Nye), набуло поширення у зв'язку з гібридними загрозами та новими формами м'якої сили.

2. QUAD – неформальний стратегічний діалог чотирьох демократичних країн Індії, США, Японії, Австралії, який із 2020-х рр. активно просуває тематику цифрової безпеки.

3. ASEAN Digital Masterplan – стратегічний документ АСЕАН (2021), що визначає бачення цифрового майбутнього регіону, формуючи цифрову інтеграцію, стандарти безпеки, стійкість до кіберзагроз.

4. Кібердипломатія – активно розвивається з 2010-х рр. у межах міжнародних організацій (ООН, ОБСЄ, ЄС), передбачає як двосторонню, так і багатосторонню взаємодію щодо управління кіберпростором.

5. Інформаційна резиліентність – концепція, що інтегрує безпековий, комунікаційний та соціальний підходи; активно використовується НАТО, ЄС, а також в національних стратегіях кібербезпеки.

6. Інформаційний вплив у зовнішній політиці АТР трансформувався з інструменту «м'якої сили» у повноцінний важіль геополітичного тиску, який реалізується через цифрову дипломатію, дезінформаційні кампанії, експансію технологічних стандартів і платформ.

7. Цифрова інфраструктура, насамперед підводні кабелі, протоколи маршрутизації (BGP) та кіберплатформи, стає ареною стратегічної конкуренції. Контроль над нею дозволяє державам посилювати або обмежувати вплив конкурентів.

8. У регіоні спостерігається фрагментація глобального Інтернету й формування альтернативних цифрових моделей: китайська (інформаційний контроль), американська (відкритість), європейська (регулювання).

9. Формується нова концепція інформаційного меркантилізму, в межах якої інформація розглядається як актив, що потребує захисту, накопичення й використання як політичного ресурсу.

10. Попри глибоку конкуренцію, держави АТР шукають баланс у вигляді цифрової співпраці через механізми QUAD, IPEF, ASEAN Digital Masterplan – як форму захисту від спільних викликів (кіберзагроз, дезінформації, технодомінування).

Таким чином, виявлено, що інформаційна резиліентність та технологічний суверенітет стають новими параметрами геополітичної сили, нарівні з військовими та економічними компонентами. Проведене дослідження вносить внесок у розвиток української школи регіональних студій, демонструючи приклад адаптації новітніх глобальних викликів до регіональної специфіки АТР.

У контексті зростання загроз цифрового авторитаризму та кібершпиунства, державам необхідно: розвивати національні стратегії цифрової дипломатії; формувати системи стійкості до інформаційного впливу; брати участь у створенні міжнародних правил цифрової взаємодії.

Література

1. Батюкова Н. О. Цифрова дипломатія як механізм забезпечення зовнішньополітичної комунікації // Нац. авіац. ун-тет. Вісник НАУ. 2021. 212 с.
2. Кабаненко І. В. Цифрова стратегія і глобальна безпека: загрози, виклики, рішення / Київ: НІСД, 2022. 68 с.
3. Казмірчук Ю. Інформаційна політика країн АТР: міждержавні виклики і національні інтереси // Укр. ж-л міжнародного права. 2023. №1. С. 21–30.
4. Кастельс М. Інформаційна ера: економіка, суспільство і культура. Т. 1: Суспільство мереж.

К.: Видавничий дім «Києво-Могилянська академія», 2004.

5. Литвиненко О. Ю. Інформаційна безпека в міжнародних відносинах: нові виклики та стратегічні пріоритети // Гілея: наук. вісник. 2020. №152(9). С. 39–43.

6. Най, Дж. М'яка сила: засоби досягнення успіху в міжнародній політиці / Джозеф Най ; пер. з англ. Київ: Основи, 2007. 204 с.

7. Сябро А. В. Трансформація пріоритетів регіональної політики у сфері інформаційної безпеки (на прикладі країн АТР). Дис. Київський національний університет ім. Тараса Шевченка, 2022.

8. Сябро А. В. Інформаційний компонент регіональної безпеки в політиці країн АТР. Схід, №3 (171), 2022. С. 59–65.

9. ASEAN Digital Masterplan 2025-ASEAN Secretariat. 2021. URL: <https://asean.org/asean-digital-masterplan-2025>; <https://asean.org/wp-content/uploads/2021/01/ASEAN-Digital-Masterplan-2025.pdf> (дата звернення: 31.05.2025)

10. Castells, M. The Rise of the Network Society. Wiley-Blackwell. 2010.

11. Cybersecurity Law of the People's Republic of China. NPC Observer. URL: <https://npcobserver.com/2016/11/07/full-translation-cybersecurity-law> (дата звернення: 03.06.2025)

12. Data Free Flow with Trust (DFFT) – Government of Japan. URL: <https://www.mofa.go.jp/policy/economy/dfft/index.html> (дата звернення: 03.06.2025)

13. Das, S. Digital Sovereignty and ASEAN: Between Great Powers and Regional Ambitions. Journal of ASEAN Studies, 2022. Vol. 10(1), P. 55–70.

14. Feigenbaum E. China and the World: Dealing with a Reluctant Global Power // Foreign Affairs. 2023. № 1. P. 45–58.

15. Fontaine R., Rogers J. The Innovation Wars: America's Quest to Maintain Technological Supremacy. Center for a New American Security, 2022. URL: <https://www.cnas.org> (дата звернення: 31.05.2025)

16. Hoffman S., Kania E. The Digital Silk Road: China's Global Technology Vision. Australian Strategic Policy Institute, 2021. URL: <https://www.aspi.org.au/report/digital-silk-road> (дата звернення: 04.06.2025)

17. Nye J. The Future of Power. New York: PublicAffairs, 2011. 320 p.

18. Nye J. Soft Power: The Means to Success in World Politics. New York: Public Affairs, 2004.

19. QUAD Joint Leaders' Statement. (2022). White House Official Documents. <https://www.whitehouse.gov> (дата звернення: 03.06.2025)

20. Shambaugh D. Where Great Powers Meet: America and China in Southeast Asia. Oxford University Press, 2020. 304 p.

21. Walker, C. The Authoritarian Threat: The Hijacking of Soft Power. Journal of Democracy, 2016, № 27(1), P. 49–63.

References

1. Batyukova N. O. (2021) Tsyfrova dyplomatiya yak mekhanizm zabezpechennya zovnishn'opolitychnoyi komunikatsiyi. Nats. Aviat. un-tet. Visnyk NAU. 212 p.

2. Kabanenko I. V. (2022) Tsyfrova stratehiya i hlobal'na bezpeka: zahrozy, vyklyky, rishennya. Kiyiv: NISD. 68 p.

3. Kazmirchuk YU. (2023) Informatsiyina polityka krayin ATR: mizhderzhavni vyklyky i natsional'ni interesy // Ukr. zh-l mizhnarodnoho prava. №1. P. 21–30.

4. Kastel's M. (2004) Informatsiyina era: ekonomika, suspil'stvo i kul'tura. T. 1: Suspil'stvo merezh. K.: Vydavn. dim «Kiyevo-Mohylyans'ka akademiya».

5. Lytvynenko O. YU. (2020) Informatsiyina bezpeka v mizhnarodnykh vidnosynakh: novi vyklyky ta stratehichni priorytety. Hileya: nauk. visnyk. №152(9). P.39-43.

6. Nay, Dzh. (2007) M'yaka syl: zasoby dosyahnennya uspihu v mizhnarodniy politytsi / Dzhozef Nay ; per. z anhl. Kyiv: Osnovy. 204 p.

7. Syabro A. V. (2022) Transformatsiya priorytetiv rehional'noyi polityky u sferi informatsiyanoi bezpeky (na prykladi krayin ATR). KNU im. T. Shevchenka.

8. Syabro A. V. (2022) Informatsiyyny komponent rehional'noyi bezpeky v politytsi krayin ATR. Skhid, №3 (171). P. 59–65.

9. ASEAN Digital Masterplan 2025–ASEAN Secretariat. 2021. URL: <https://asean.org/wp-content/uploads/2021/01/ASEAN-Digital-Masterplan-2025.pdf> (accessed May 31, 2025)

10. Castells, M. (2010) The Rise of the Network Society. Wiley-Blackwell.

11. Cybersecurity Law of the People's Republic of China. NPC Observer. URL: <https://npcobserver.com>

com/2016/11/07/full-translation-cybersecurity-law (accessed June 03, 2025)

12. Data Free Flow with Trust (DFFT) - Government of Japan. URL: <https://www.mofa.go.jp/policy/economy/dfft/index.html> (accessed June 03, 2025)

13. Das, S. (2022) Digital Sovereignty and ASEAN: Between Great Powers and Regional Ambitions. *Journal of ASEAN Studies*, 10(1), P. 55–70.

14. Feigenbaum E. (2023) China and the World: Dealing with a Reluctant Global Power // *Foreign Affairs*. № 1. P. 45–58.

15. Fontaine R., Rogers J. (2022) The Innovation Wars: America's Quest to Maintain Technological Supremacy. Center for a New American Security. URL: <https://www.cnas.org> (accessed May 31, 2025)

16. Hoffman S., Kania E. (2021) The Digital Silk Road: China's Global Technology Vision. Australian Strategic Policy Institute. URL: <https://www.aspi.org.au/report/digital-silk-road> (accessed June 04, 2025)

17. Nye J. (2011) *The Future of Power*. New York: PublicAffairs. 320 p.

18. Nye J. (2004) *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

19. QUAD Joint Leaders' Statement. (2022). White House Official Documents. <https://www.whitehouse.gov> (accessed June 03, 2025)

20. Shambaugh D. (2020) *Where Great Powers Meet: America and China in Southeast Asia*. Oxford University Press. 304 p.

21. Walker, C. (2016). The Authoritarian Threat: The Hijacking of Soft Power. *Journal of Democracy*, 27(1), P. 49-63.