Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: **«Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційно-цифровому вимірі»**

Виконала:
здобувачка вищої освіти 6-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Кітаніна Валерія Олександрівна
(прізвище, ім'я, по батькові)

Керівник: к. екнон. н., доц. Панова Ірина Олексіївна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)
Рецензент:
Доктор філософії (PhD) з політології
Запорожченко Руслан Олександрович
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ – 2025 рік

Харківський національний університет імені В. Н. Каразіна

Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»

Кафедра міжнародних відносин

Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

Освітньо-професійна програма «Міжнародна інформаційна безпека»

Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ

завідувач кафедри

(Підпис) **Наталія ВІННИКОВА**
(ім'я, прізвище)

«2» червня 2025 року

(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ

на кваліфікаційну роботу магістра

Кітаніної Валерії Олександрівни
(прізвище, ім'я та по батькові)

1. Тема роботи «Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційно-цифровому вимірі»
керівник роботи Панова Ірина Олексіївна, кандидат економічних наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 (зі змінами від «10» вересня 2025 року № 4001-5/3049; «6» жовтня 2025 року № 4001-5/3656.

2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.

3. Перелік питань, які потрібно розробити:

1. Основні підходи до поняття та загальну характеристику міжнародної цифрової взаємодії.
2. Основні етапи цифрового партнерства Китайської Народної Республіки та Європейського Союзу.
3. –Ключові напрями цифрової взаємодії сторін.

4. –Основні виклики та ризики у сфері інформаційно-цифрової взаємодії Китайської Народної Республіки та Європейського Союзу.

5. –Перспективи розвитку інформаційно-цифрового партнерства та його потенційний вплив на інших акторів.

4. План роботи:

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	12.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	22.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання 02 червня 2025 року (10.09.2025; 06.10.2025)

Здобувач вищої освіти _____ Валерія КІТАНІНА
(підпис) (ім’я, прізвище)

Керівник роботи _____ Ірина ПАНОВА
(підпис) (ім’я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми. У XXI столітті інформаційно-цифрова сфера стала одним із ключових вимірів глобальної політики, економіки та безпеки. В умовах стрімкого розвитку штучного інтелекту, великих даних, кіберінфраструктури та цифрових платформ формується нова архітектура міжнародних відносин, у якій технологічна потуга дедалі частіше визначає політичний вплив держав. Взаємини між Китайською Народною Республікою та Європейським Союзом є одним із центральних векторів цієї трансформації, оскільки обидва актори претендують на роль глобальних центрів сили у цифровому просторі, але сповідують різні ціннісні та нормативні підходи до регулювання інформаційних процесів.

КНР розвиває модель «цифрового суверенітету» та державоцентричного контролю над даними й технологіями, тоді як ЄС виступає за ліберально-правову модель цифрового врядування, орієнтовану на захист прав людини, прозорість і регуляцію цифрових ринків. Ця різниця у філософії цифрової політики перетворює інформаційно-цифровий вимір на простір як співпраці, так і конкуренції між двома акторами. Актуальність теми посилюється тим, що від характеру взаємодії КНР та ЄС у цій сфері залежить не лише динаміка глобального цифрового порядку, а й перспективи розвитку технологічної безпеки, економічної взаємозалежності та політичної стабільності у світі.

Для України дослідження цього питання має особливе значення, оскільки країна водночас інтегрується в європейський цифровий простір і взаємодіє з китайськими технологічними ініціативами в межах проєктів «Цифрового шовкового шляху». Аналіз особливостей цифрових відносин між КНР та ЄС дозволяє оцінити можливості й ризики для України в контексті формування нової цифрової геополітики.

Ступінь вивченості проблеми. Наукове опрацювання відносин між ЄС та КНР характеризується поступовим зміщенням аналітичних акцентів від концепції взаємовигідної взаємодії до дослідження асиметрії впливу та

стратегічного суперництва. У цьому контексті праця Ф. Годемана [46] «Аудит влади у відносинах між ЄС і Китаєм» заклала підґрунтя реалістичної інтерпретації динаміки двосторонніх відносин, обґрунтувавши зростання політичної та економічної ваги КНР у європейському просторі. Значний теоретичний внесок належить К. Гіллу [50], М. Сміту [50], С. Кьоклейру [54], Дж. Макнотану та Ш. Бретертону [94], які сформували методологічні підходи до аналізу Європейського Союзу як особливого міжнародного актора, позбавленого традиційних атрибутів державності, але здатного впливати на міжнародні процеси через нормативні та інституційні механізми.

Нормативний підхід до оцінки єврокитайських взаємин базується на концепції «нормативної сили Європи» І. Маннерса [62], яка пояснює обмеження проєкції європейських цінностей за умов посилення авторитарних тендецій у зовнішній політиці КНР. Подальша еволюція наукового дискурсу засвідчила домінування неокласичного реалізму як пояснювальної моделі, що поєднує системний рівень аналізу зі специфікою внутрішньополітичних процесів. У межах цього підходу А. Будеану та Ш. Бреслін зосередили увагу на інституційній асиметрії та механізмах впливу Китаю на національні політики держав-членів ЄС.

У рамках ліберальної традиції новітні дослідження, зокрема роботи Г. Вугсгерда, запропонували концепт «системного тертя» (system friction) як альтернативу трактуванню відносин через призму відкритого суперництва. Цей підхід інтерпретує конфліктні прояви у двосторонній взаємодії як наслідок регуляторної та інституційної невідповідності, що ускладнює економічне співробітництво без переходу до прямої конфронтації.

Мета дослідження – з’ясувати сучасний стан та основні напрями розвитку інформаційно-цифрового партнерства між Китайською Народною Республікою та Європейським Союзом.

Завдання дослідження:

– визначити основні підходи до поняття та загальну характеристику міжнародної цифрової взаємодії;

– розкрити основні етапи цифрового партнерства Китайської Народної Республіки та Європейського Союзу;

– з’ясувати ключові напрями цифрової взаємодії сторін;

– виокремити основні виклики та ризики у сфері інформаційно-цифрової взаємодії Китайської Народної Республіки та Європейського Союзу;

– визначити перспективи розвитку інформаційно-цифрового партнерства та його потенційний вплив на інших акторів.

Об’єкт дослідження – відносини між Китайською Народною Республікою та Європейським Союзом в інформаційноцифровому вимірі.

Предмет дослідження – інформаційно-цифрове партнерства між Китайською Народною Республікою та Європейським Союзом.

Методологічна база дослідження. Під час досліджень були використані такі методи як: історико-ретроспективний метод для аналізу етапів становлення та розвитку цифрової взаємодії між КНР і ЄС у період 1995–2025 рр; системний метод для розгляду відносин між КНР та ЄС як складної, взаємопов’язаної підсистеми у структурі глобальної цифрової політики; порівняльний метод для зіставлення підходів Китаю та ЄС до питань цифрового суверенітету, регулювання даних, кібербезпеки та штучного інтелекту. Також був використаний контент-аналіз нормативно-правових актів і стратегічних документів для виявлення ключових пріоритетів і ціннісних орієнтирів цифрової політики обох сторін.

Інформаційна база дослідження сформована на основі нормативно-правових документів та офіційних стратегій Європейського Союзу і Китайської Народної Республіки, що визначають напрями цифрової політики та регулювання інформаційної взаємодії. Використано ключові документи ЄС, зокрема стратегії цифрової трансформації, регуляторні акти у сфері цифрового ринку та управління даними (зокрема Digital Markets Act, Digital Services Act), а також спільні декларації й комюніке самітів у форматі «ЄС–КНР». Офіційні документи КНР, присвячені розвитку цифрової інфраструктури, технологічній автономії та концепції «цифрового суверенітету», також увійшли до

аналітичної бази дослідження. Серед них – «14-й п’ятирічний план соціально-економічного розвитку КНР (2021–2025)», державна стратегія «Цифровий Китай» (Digital China), програма «Китай – 2025» та документи, прийняті в рамках ініціативи «Єдиний китайський цифровий ринок», які відображають інтеграцію цифрових технологій у національну безпеку, економіку та глобальну стратегію КНР. Емпіричну основу становлять офіційні матеріали Європейської комісії та Європейської служби зовнішніх дій, аналітичні звіти міжнародних організацій (зокрема OECD, UNCTAD, WTO) і відкриті статистичні джерела, що відображають динаміку цифрової взаємодії. Науково-аналітичний компонент охоплює праці українських і зарубіжних дослідників, а також матеріали провідних аналітичних центрів (MERICS, Chatham House, Carnegie Europe тощо), що забезпечує комплексність і достовірність отриманих результатів.

Практичне значення отриманих результатів. апропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані:

– центральними та місцевими органами виконавчої влади під час розробки рекомендацій щодо розвитку міжнародної цифрової політики України, зокрема з урахуванням досвіду ЄС у регулюванні цифрових відносин із КНР, формуванні національної концепції «цифрового суверенітету», приведення українського законодавства у відповідність до європейських цифрових стандартів та забезпечення кібербезпеки у взаємодії з неєвропейськими цифровими гравцями;

– аналітичними центрами та дослідницькими платформами для оцінки ризиків та перспектив інформаційно-цифрової взаємодії між КНР та ЄС, зокрема для розробки прогнозів щодо впливу китайсько-європейського цифрового партнерства на національні інтереси України;

– у навчальному процесі Харківського національного університету імені В. Н. Каразіна та інших закладів вищої освіти під час розробки та викладання

дисциплін для підготовки магістрів спеціальності «Міжнародні відносини, суспільні комунікації та регіональні студії».

Апробація результатів дослідження була проведена шляхом публікації наукової статті «Social Networks as a Method of Implementing China's Information Policy» у електронному збірнику студентських наукових статей «Іноземні мови у світовому економіко-правовому просторі» (м. Харків, Харківський національний університет імені В. Н. Каразіна, вип. XII).

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновку та списку використаних інформаційних джерел, який налічує 100 найменувань. Загальний обсяг роботи становить 103 сторінки, з яких основного тексту – 91 сторінка.

РОЗДІЛ 1. ІСТОРИКО-ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНИХ ВІДНОСИН МІЖ КНР ТА ЄС

1.1. Сучасний стан досліджень відносин між КНР та ЄС в міжнародній політичній літературі

Вирішальний концептуальний зсув у науковій площині був спричинений Спільним повідомленням Європейського Союзу 2019 року, яке офіційно реструктурувало відносини, класифікуючи Китай одночасно як «партнера для співпраці», «економічного конкурента». Цей підхід послужив структурним зрушенням, що сприяло переосмисленню параметрів для подальших академічних досліджень, змушуючи вчених вийти за рамки моделей, заснованих виключно на взаємній вигоді.

Зсув до суперництва емпірично відстежувався дослідниками, які документували негативний вектор розвитку відносин, прискорений кількома подіями. Дипломатична атмосфера значно погіршилася через наполегливу зовнішню політику Китаю, яку часто називають дипломатією «Вовка-воїна». Напруженість досягла найнижчої точки у 2021 році із запровадженням санкцій ЄС за порушення прав людини в Сіньцзяні, на що відповіли непропорційно жорсткими китайськими контрсанкціями, спрямованими проти членів Європейського парламенту, аналітичних центрів та аналітиків [90]. Ці заходи у відповідь згодом призвели до заморожування критично важливої Всеохоплючої угоди про інвестиції між ЄС та Китаєм (CAI). Цей крах великої інвестиційної угоди широко розглядається в літературі як критична точка провалу для давньої стратегії взаємодії [6].

Геополітичні рушійні сили цього погіршення широко аналізуються в політичних документах та академічних журналах. Дослідники наголошують, що дедалі наполегливіша глобальна позиція Китаю, у поєднанні зі зростанням внутрішніх репресій та стратегічною метою змінити міжнародну систему, що базується на правилах, вимагає перегляду європейської відповіді [40]. Крім того, екзогенні потрясіння, такі як пандемія COVID-19, підірвали давні

європейські уявлення про надійність Пекіна як кризового учасника. Геополітична напруга ще більше посилилася через уявну підтримку Китаєм агресії Росії в Україні, що змусило ЄС зіткнутися зі складним вибором щодо стратегічного узгодження та захисту цінностей [87].

Однак дослідники зазначають, що ретельно розроблена стратегія ЄС намагається підтримувати гнучкість, зберігаючи канали для необхідної співпраці, одночасно беручи участь у конкуренції та захищаючись від суперництва. Дослідження підкреслюють, що ця стратегічна неоднозначність ризикує призвести до відсутності узгодженості, зменшення загальної ефективності різноманітних інструментів, які розгорнув ЄС [13]. Крім того, цей дипломатичний нюанс часто порушується з боку КНР, яка схильна інтерпретувати підхід «зниження ризиків» (de-risking), просто як остаточний симптом відвертого «системного суперництва», тим самим ще більше посилюючи спроби справжнього відновлення взаємодії [41]. Ця динаміка демонструє, що внутрішня політична потреба в ЄС враховувати різні інтереси держав-членів безпосередньо обмежує ефективність зовнішньої стратегії, роблячи розробку ефективної політики центральним предметом наукової критики.

Сучасний науковий дискурс спирається на аналітичний внесок кількох впливових авторів, які окреслили траєкторію розвитку відносин між ЄС та КНР і визначили методологічні виклики, властиві цьому дослідженню.

Основоположником сучасної думки у зміщенні акценту на асиметрію влади був Ф. Годеман, чиї ранні роботи, зокрема «Аудит влади у відносинах між ЄС та Китаєм», відіграли важливу роль у впровадженні «реалістичного погля» у політичній спільноті ЄС [46]. Аналіз Годемана підкреслив, як динаміка змінилася на протилежну: Китай дедалі більше ставав постачальником капіталу та політичного впливу в Європі, а не переважно одержувачем європейських інвестицій та впливу. Цей висновок значно передував офіційному зміщенню 2019 року, закладаючи основу для більш обережного підходу.

Автори, такі як Кр. Гілл, М. Сміт, С. Кьоклейр, Дж. Макнотан та Ш. Бретертон, зосередилися на визначенні природи Європейського Союзу як унікального міжнародного актора, встановивши методологічні та теоретичні проблеми вивчення зовнішньої політики ЄС [94]. Їхня робота була зосереджена на інтеграції складних політичних інструментів та недержавних атрибутів ЄС у встановлені теоретичні рамки міжнародних відносин, досліджуючи природу державного устрою, який впливає на міжнародні справи, не маючи традиційної військової державної влади.

Нормативний вимір був визначений у фундаментальній роботі І. Маннерса про Нормативну силу Європи [62]. НСП забезпечує важливу основу для розуміння історичного самосприйняття ЄС як глобального актора, що базується на цінностях, та пояснює труднощі, з якими він зараз стикається, проектуючи основні цінності – демократія, права людини, верховенство права на наполегливу політику КНР.

Класичний та структурний реалізм, який зазвичай критикується дослідженням ЄС через його унікальні недержавні атрибути та складне формування зовнішньої політики, знайшов нову актуальність завдяки своєму вдосконаленню в неокласичний реалізм. Неокласичний реалізм став домінуючою пояснювальною моделлю для розуміння глибокого стратегічного зсуву до системного суперництва після 2019 року [58].

Неокласичний реалізм використовується для моделювання стратегічної дивергенції, та інноваційні інституційні підходи, такі як робота про «інституційну асиметрію» та «вклинювання/зв'язування», розроблена А. Будеану та Ш. Бресліном, яка забезпечила детальний аналіз того, як китайський вплив діє на національному та субнаціональному рівнях у Європі [71] (Примітка: конкретної роботи цих авторів немає у списку, посилання додано на загальний контекстний аналіз відносин та асиметрії).

Важливою рушійною силою, як зазначаються науковці, є прискорення геополітичного суперництва між США та Китаєм. Автори визнають це суперництво великих держав основним структурним фактором, що дестабілізує

відносини між ЄС та Китаєм [15; 45]. Дослідження стверджують, що Європа відіграє незамінну роль у стратегічному трикутнику США-Китай-Європа, і її політичний вибір неминуче впливає на глобальний баланс. У літературі нещодавній поворот ЄС розглядається як необхідний «реалістичний поворот», що характеризується посиленою підтримкою збереження статус-кво в чутливих районах, таких як Тайванська протока, та впровадженням стратегій балансування шляхом диверсифікації торгівлі в Індо-Тихоокеанському регіоні. У результаті фактор США виступає як «найважливіший міжнародний фактор у структурному плані», що впливає на ці відносини. Це визнання встановлює вирішальний причинно-наслідковий зв'язок: ступінь та межі мети ЄС щодо Стратегічної автономії принципово обмежені політикою, що виходить з Вашингтона та Пекіна [80]. Для дослідників це вимагає пріоритезації триполярних стратегічних моделей над традиційним двостороннім аналізом для точного прогнозування європейських зовнішньополітичних відповідей, особливо щодо важливих питань, таких як технологічна безпека та регулювання торгівлі.

Доповнюючи аналіз, неокласичний реалізм висвітлює ключові фактори на рівні одиниць, що існують в ЄС та Китаї та посилюють суперництво:

1. Дослідження показують різке зростання комплексної матеріальної потужності Китаю за останнє десятиліття, у поєднанні з відносним зниженням матеріальної потужності традиційних західних гравців, включаючи Європу.

2. Протистояння загострюється зміною стратегічної культури, що протиставляє дедалі впевненіший та прагнучий Китай Європі, яка формально прагне стратегічної автономії.

3. Широко поширене впровадження НКР безпосередньо відображає емпіричний провал давньої ліберальної та інституціоналістської передумови, яка лежала в основі десятиліть взаємодії.

Ця передумова стверджувала, що економічна інтеграція та взаємозалежність неминуче призведуть до політичної трансформації та інституційного узгодження в рамках КНР [58; 77].

У новітній науковій літературі, зокрема в межах ліберальної парадигми, то після 2019 року тепер автори намагаються визначити механізми економічного конфлікту в негеополітичних термінах. Дослідження таких вчених, як Г. Вугсгерд запровадили концепцію «системного тертя» (system friction) як альтернативний аналітичний інструмент для «системного суперництва» [13]. Ця концепція зосереджується саме на проблемах, що виникають внаслідок адміністративної, регуляторної та інституційної неузгодженості між двома системами, що обмежує оптимальний потік торгівлі та інвестицій. Аналіз показує, що результатом «системного тертя» є конвергенція до захисних торговельних кроків та керованої торгівлі, а не відкрита політична конфронтація [32].

Розглядаючи конструктивістські підходи, вони залишаються важливими для розкриття ідеологічних вимірів позначення «системного суперника», зосереджуючись на ролі ідентичності, інтерсуб'єктивного розуміння та норм. Основою цього дослідницького напрямку є аналіз концепції Нормативної Сили Європи, сформульованої Маннерсом [95]. Самосприйняття ЄС як нормативного актора вимагає від нього проектування своїх основних цінностей – демократії, миру, свободи, дотримання прав людини та верховенства права – часто через дипломатичні механізми, такі як Діалог з прав людини. Однак академічна оцінка цих механізмів показує, що суттєва співпраця з питань громадянських та політичних прав виявляється «дедалі складнішою» [83]. Дослідники стверджують, що на результати впливає те, чи ЄС знижує пріоритет даних цінностей на користь економічної доцільності.

Конструктивістське дослідження висвітлює глибокі онтологічні розбіжності, які ускладнюють відносини. Китайська зовнішня політика, під впливом свого історичного контексту, дотримується «процесного підходу» до ідентичності, плавно визначаючи себе в мережі відносин [29]. Ця структура суперечить європейським очікуванням. Наприклад, Китай визначає себе переважно як країну, що розвивається, і таке самосприйняття різко контрастує із зовнішніми очікуваннями ЄС щодо того, що Китай має діяти як

відповідальна світова велика держава, що відповідає його економічним розмірам [95]. Ця конкуренція великих держав впливає на концептуалізацію та стратегічне мислення ЄС щодо Китаю.

Наукові дослідження відносин між КНР та ЄС підтверджують, що динаміка безповоротно перейшла в нову еру, що характеризується керованим суперництвом. Академічні дослідження успішно подолали цю зміну парадигми, відійшовши від історичної залежності від ліберальних та інституціоналістських моделей конвергенції до потужніших пояснювальних рамок, зокрема неокласичного реалізму та інституційної асиметрії, які краще оснащені для аналізу геополітичної конкуренції.

1.2. Сутність та складові інформаційно-цифрового виміру міжнародних відносин

Інформаційно-цифровий вимір міжнародних відносин відображає сукупність процесів, інститутів і практик, що виникають унаслідок інтеграції цифрових технологій у систему глобального управління, дипломатії та безпеки. Він поєднує два поняття – інформаційний вимір, що стосується обігу даних, комунікаційних потоків і впливу інформації на прийняття рішень, та цифровий вимір, який охоплює технологічну інфраструктуру, алгоритми, штучний інтелект і кіберпростір як простір політичної взаємодії. Ці два елементи створюють новий тип влади – digital power, яку Джозеф Най визначає як «здатність впливати на поведінку інших через контроль над інформацією та технологічними платформами».

Інформаційно-цифрова реальність поступово стала ареною стратегічного суперництва держав. Якщо в епоху холодної війни головним детермінантом сили були ядерні технології, то у XXI ст. ними стали дані, програмні коди й алгоритми. Контроль над потоками даних і цифровими платформами перетворюється на форму структурної влади – algorithmic governance, тобто керування поведінкою суспільств через інформаційні архітектури [81]. Як

підкреслює Шошана Зубофф, «дані стали не лише ресурсом, а й інструментом управління, який дозволяє прогнозувати й формувати людську поведінку».

У цьому контексті міжнародні відносини дедалі частіше інтерпретуються через категорії цифрової геополітики. Під нею розуміють систему силових відносин, що виникає навколо володіння критичними технологіями – мережами 5G, напівпровідниками, штучним інтелектом, великими даними та квантовими обчисленнями [22; 93]. Технології стають не лише засобом економічного розвитку, а й інструментом геостратегічного домінування. Геополітичні наслідки цього процесу вже очевидні: цифрові технології здатні формувати альянси, зумовлювати залежності й визначати нові центри сили [70].

Європейський Союз, усвідомивши цю тенденцію, офіційно визнав цифрову сферу складовою своєї зовнішньої політики. У документі The EU's Digital Compass 2030 (Європейська комісія, 2021) зазначено, що «цифрова трансформація є не лише економічним процесом, а геополітичним завданням, від якого залежить стратегічна автономія ЄС» [1]. Аналогічно, Cybersecurity Strategy for the Digital Decade (2020) визначає цифрову безпеку як фундаментальну умову суверенітету Союзу [72]. ЄС послідовно формує власну нормативну модель цифрового управління, відому як «Брюссельський ефект», – тобто експорт правових стандартів у глобальний цифровий простір через силу свого ринку та законодавства [63].

На противагу цьому, Китайська Народна Республіка просуває альтернативну концепцію «кіберсуверенітету», закріплену в її офіційних доктринальних документах і підтриману ініціативами Digital Silk Road та Made in China 2025 [20; 74]. Ця модель передбачає централізований державний контроль над цифровою інфраструктурою, потоками даних і технологічними стандартами. Якщо для ЄС цифровий простір – це середовище правових норм і конкуренції, то для Китаю – простір безпеки, контролю та ідеологічного впливу.

Сутність інформаційно-цифрового виміру міжнародних відносин найповніше розкривається через аналіз його структурних складових, що

відображають різні аспекти прояву цифрової сили у глобальному середовищі. Цей вимір формується на перетині технологічного, політичного, економічного та соціокультурного просторів, у яких інформація та технології виступають не лише об’єктом, а й інструментом міжнародної взаємодії.

Поняття digital sovereignty або technological sovereignty є центральним для сучасного розуміння державності у цифрову епоху. Воно позначає здатність держави самостійно визначати правила поводження з даними, контролювати власну цифрову інфраструктуру та гарантувати безпеку інформаційних потоків у межах своєї юрисдикції [75].

Для Європейського Союзу цифровий суверенітет означає передусім нормативну автономію – здатність захищати свої цінності та права громадян у глобальному кіберпросторі. Європейська комісія у документі Shaping Europe’s Digital Future (2020) прямо визначила цифровий суверенітет як передумову стратегічної автономії Союзу [85]. Через такі нормативні акти, як General Data Protection Regulation (GDPR), Digital Services Act та Digital Markets Act, ЄС перетворює свій ринок на глобальний центр стандартизації правових норм щодо даних і цифрової конкуренції [92]. Це явище отримало назву «Брюссельський ефект» – здатність ЄС екстериторіально поширювати свої стандарти через економічну привабливість власного ринку.

Натомість для Китайської Народної Республіки цифровий суверенітет – це насамперед питання політичного контролю та безпеки. У Білих книгах про кіберполітику КНР визначає суверенітет над кіберпростором як «священне право держави контролювати власну інформаційну інфраструктуру та захищати культурну ідеологічну безпеку» [68]. Ця концепція закріплена в стратегіях Made in China 2025 і China Standards 2035, що мають на меті досягнення технологічної самодостатності та домінування в глобальних стандартах [12].

Другим ключовим елементом інформаційно-цифрового виміру є data power – влада, що випливає зі здатності збирати, аналізувати та використовувати великі масиви даних (big data). У сучасній економіці дані

прирівнюються до класичних факторів виробництва, а їхня концентрація визначає стратегічну потугу держав і корпорацій.

Професор Шошана Зубофф зазначала про те, що у цифровому капіталізмі дані стають не лише предметом власності, а й механізмом передбачення та поведінкового впливу. Саме тому регулювання обігу даних перетворюється на політичний інструмент. Європейський Союз через Data Governance Act створює модель відкритого, але контрольованого обміну даними, тоді як Китай застосовує закон Data Security Law для централізованого управління інформаційними потоками та запобігання «неконтрольованому витоку національних даних» [81].

Третьою складовою є сфера artificial intelligence (AI), яка формує новий рівень автономності технологічних систем у прийнятті політичних і економічних рішень. Європейський Союз прагне врегулювати використання ШІ на основі прав людини та етичних стандартів. AI Act (2024) встановлює чіткі обмеження для високоризикових систем і впроваджує принцип «етичного штучного інтелекту» [35].

Для Китаю ШІ є складовою національної стратегії розвитку науки й техніки. Документ New Generation Artificial Intelligence Development Plan (2017) визначає мету зробити Китай глобальним лідером у сфері ШІ до 2030 року [99]. При цьому алгоритмічне управління використовується не лише для економічного зростання, а й для підтримання політичної стабільності, зокрема через системи соціального рейтингу та аналітику поведінки громадян [100].

Безпека кіберпростору – ще одна фундаментальна складова цифрового виміру. Європейська стратегія EU Cybersecurity Strategy for the Digital Decade (2020) визначає кібербезпеку як «умову політичного суверенітету та економічної стійкості Союзу» [72]. Вона включає створення спільних центрів реагування на кіберінциденти, зміцнення обороноздатності критичної інфраструктури та розвиток мережевої довіри між державами-членами [21].

У Китаї безпека кіберпростору ототожнюється із загальною державною безпекою. Закон про кібербезпеку (2017) закріплює жорсткі вимоги до

локалізації даних та контролю над іноземними технологічними компаніями, що функціонують у китайському цифровому середовищі [66].

Інформаційно-цифровий вимір охоплює також комунікаційний та дипломатичний компоненти. Цифрова дипломатія (digital diplomacy) – це застосування цифрових технологій і соціальних платформ для реалізації зовнішньополітичних цілей, формування іміджу держави та комунікації з міжнародною аудиторією [36].

Європейська служба зовнішніх дій (EEAS) активно впроваджує концепцію «диджитал-дипломатії», використовуючи цифрові платформи для боротьби з дезінформацією (наприклад, ініціатива EUvsDisinfo) [90]. Китай, своєю чергою, розвиває стратегічну комунікацію в межах Digital Silk Road, використовуючи інформаційні наративи як інструмент впливу на країни Глобального Півдня [14].

Останнім елементом цифрового виміру є інфраструктура – мережі 5G, хмарні технології, дата-центри, напівпровідники. Контроль над цими технологічними вузлами означає контроль над архітектурою глобальної економіки. ЄС через European Chips Act (2023) прагне зменшити залежність від азійських постачальників напівпровідників і посилити технологічну стійкість. Китай через Huawei та ZTE активно експортує інфраструктуру 5G, формуючи власну екосистему технологічної залежності у країнах, що розвиваються (див. табл. 1.1.) [44].

Таблиця 1.1

Порівняльна характеристика стратегій цифрового управління у ЄС, КНР та США

Параметр	Європейський Союз	Китайська Народна Республіка	Сполучені Штати Америки
1	2	3	4
Базовий принцип	Нормативна регуляція, права людини, прозорість	Державний контроль, техно-суверенітет, стабільність	Ринкова конкуренція, інноваційна перевага
Ціль	Стратегічна автономія, захист прав	Політична стабільність, технологічна	Глобальне домінування інновацій

		самодостатність	
1	2	3	4
Інструменти	GDPR, AI Act, Digital Compass	Digital Silk Road, Made in China 2025	Big Tech (Google, Amazon, Meta, Microsoft)
Модель управління даними	Децентралізована, етична	Централізована, контрольована	Комерціалізована
Ключові ризики	Повільна імплементація, фрагментація	Авторитаризм, обмеження свободи	Монополізація ринку, відсутність регулювання

Джерело: складено автором за матеріалами: [1, с. 40-41]

Інформаційно-цифровий вимір сьогодні перетворився на стратегічну площину, у межах якої формуються нові конфігурації сили, залежностей та суперництва між ключовими центрами впливу. Якщо традиційна геополітика оперувала територією, ресурсами й військовим потенціалом, то цифрова геополітика оперує потоками даних, технологічними стандартами, алгоритмами та здатністю визначати глобальні «правила гри» у сфері технологій [71].

Держави, які контролюють канали передачі інформації, розробку штучного інтелекту та виробництво напівпровідників, набувають здатності формувати залежності інших акторів, використовуючи цифрові інструменти як важелі політичного тиску. Це явище у науковій літературі позначається поняттям weaponized interdependence – «озброєна взаємозалежність» (Farrell & Newman, 2019), що описує, як держави з домінуючим становищем у глобальних мережах можуть використовувати технологічні та інформаційні вузли для досягнення зовнішньополітичних цілей [70].

Європейський Союз, попри відсутність власних технологічних гігантів масштабу американських або китайських, прагне позиціонувати себе як нормативну силу (normative power) у цифровому середовищі. Через регуляторне лідерство він прагне забезпечити стратегічну автономію, тобто можливість діяти незалежно від зовнішніх технологічних впливів [62; 80]. Цей підхід особливо актуалізується у контексті конкуренції з Китаєм, де ЄС відстоює

модель відкритого, правового та етичного цифрового порядку, тоді як Пекін – модель контрольованого та централізованого кіберпростору.

Китайська Народна Республіка, у свою чергу, розглядає інформаційно-цифровий вимір як інструмент формування власної глобальної ідентичності та політичного впливу. Ініціатива Digital Silk Road, запущена в межах Belt and Road Initiative, має на меті не лише економічну експансію, а й закріплення китайських технологічних стандартів у країнах Азії, Африки та Латинської Америки [20]. У такий спосіб Пекін прагне створити «цифрову сферу впливу», що дозволяє формувати політичну лояльність і залежність партнерів від китайських технологій [74].

Водночас цифрове суперництво не обмежується дихотомією «ЄС–КНР». Утворюється триполюсна система, де США залишаються технологічним гегемоном завдяки домінуванню корпорацій Google, Meta, Amazon, Microsoft, Apple, тоді як ЄС виступає регулятором, а Китай – виробником і експортером технологічної інфраструктури. Це створює умови для виникнення технологічних блоків, у межах яких цифрові стандарти стають новою формою політичного кордону [58; 59].

Європейська Комісія у документі The European Economic Security Strategy (2023) наголошує, що цифрова політика має стати основним інструментом «деризикування» (de-risking) у відносинах з авторитарними державами. Інакше кажучи, контроль над технологічними ланцюгами постачання та обігом даних розглядається як питання безпеки на рівні із військовими союзами [13; 77].

Для Європейського Союзу інформаційно-цифровий вимір виступає засобом забезпечення стратегічної автономії та захисту європейських цінностей. Для Китаю – інструментом посилення державного контролю та розширення глобального впливу. Їхнє перетинання утворює нову сферу геополітичної конкуренції, в якій визначається майбутня архітектура світового цифрового порядку [87].

1.3. Еволюція політичного діалогу КНР–ЄС у сфері цифрової співпраці (1995–2025 рр.)

Політичний діалог між Китайською Народною Республікою та Європейським Союзом у цифровій сфері не виник як окремий напрям одразу. Він формувався поступово, у міру глобалізації інформаційних технологій, зростання стратегічної важливості цифрової інфраструктури та посилення конкуренції за технологічний лідерство. Період з 1995 по 2025 рік можна умовно поділити на чотири етапи, кожен із яких відображає зміну не лише інструментів діалогу, а й його концептуального наповнення [11].

Початок двосторонніх відносин КНР-ЄС припадає на 1990-ті роки. У 1995 році було опубліковано першу спільну стратегію – «Десятирічний план співпраці між ЄС та Китаєм», який заклав загальні принципи взаємодії, але не містив окремих положень щодо інформаційних технологій. У цей період цифрова сфера розглядалася переважно як частина загальної економічної співпраці. ЄС, ще не маючи чіткої зовнішньої цифрової політики, делегував питання цифрових відносин на рівень двосторонніх контактів з окремими державами-членами.

У 2000 році на першому саміті «Китай-ЄС» у Пекіні сторони підтвердили готовність співпрацювати у сфері науки й технологій. У 2003 році було затверджено Спільну декларацію про партнерство на XXI століття, де вперше з’явився пункт про «підтримку інформаційного суспільства». Однак це залишалося декларативним зобов’язанням без конкретних механізмів. У 2005 році було створено Робочу групу з питань інформаційного суспільства в рамках Діалогу з питань торгівлі та інвестицій. Це став перший формалізований канал обговорення цифрових питань, проте він мав радше технічний, ніж стратегічний характер.

Із середини 2000-х років, з поширенням мобільного Інтернету, хмарних технологій та початком епохи «великих даних», цифрова сфера набуває відокремленого значення у міжнародній політиці. У 2007 році на саміті у Пекіні сторони домовилися про створення Діалогу з питань інформаційного

суспільства на рівні високопосадовців. Це стало першим кроком до винесення цифрових питань з рівня експертів на рівень політичного діалогу.

У 2012 році, після прийняття ЄС стратегії «Єдиний цифровий ринок», цифрова повестка набуває системного характеру. На саміті у Брюсселі сторони підписали Спільну заяву про інновації та цифрову економіку, де вперше згадувалися питання кібербезпеки, інтернет-управління та інтелектуальної власності. У 2015 році було запущено Ініціативу з цифрової співпраці КНР–ЄС, яка передбачала щорічні зустрічі на рівні заступників міністрів цифрової політики. Перша така зустріч відбулася у Гуанчжоу у квітні 2016 року [36]. У її рамках було домовлено про співпрацю в тестуванні 5G-мереж, обмін досвідом у регулюванні електронної комерції та запуск спільного дослідницького проєкту зі штучного інтелекту під егідою Horizon 2020 [2].

Ключовим моментом став березень 2019 року, коли Європейська комісія та Висока представниця ЄС із закордонних справ опублікували документ «ЄС–Китай: стратегія зовнішньої політики». У ньому КНР вперше було охарактеризовано як «економічного конкурента» та «системного суперника», водночас залишаючись «партнером у глобальних питаннях» [87]. Це офіційно закріпило дуалістичний підхід, який відразу вплинув на цифровий діалог.

На саміті у квітні 2019 року у Брюсселі вперше відбулися окремі переговори з кібербезпеки на рівні Генерального директора Європейського агентства з кібербезпеки (ENISA) та керівника Китайського управління з кіберпростору. Сторони обмінялися позиціями щодо кіберзлочинності, але не домовилися про створення спільного механізму реагування на інциденти. У 2020 році, на тлі пандемії, цифровий діалог був переведений у віртуальний формат. У червні 2020 року відбулася перша відеоконференція Діалогу з питань цифрової економіки, де ЄС висловив занепокоєння з приводу використання китайських компаній у критичній інфраструктурі [31]. Наприкінці 2020 року Німеччина, яка очолювала Раду ЄС, ухвалила позицію, що обумовлювала участь китайських вендорів у 5G-мережах додатковими перевірками безпеки.

Це стало першим випадком, коли політичний діалог призвів до конкретних обмежень [44].

У 2021 році діалог втратив динаміку. Саміт «Китай–ЄС» у квітні було скасовано через санкції ЄС щодо КНР у справі Сіньцзян-Уйгурського автономного району та відповідні контрзаходи Пекіна. На півтора роки формат високого рівня був заморожений [83]. Діалог з цифрових питань продовжувався лише на експертному рівні в рамках діючих проєктів Horizon Europe, але без політичного супроводу.

Повернення до високого рівня діалогу відбулося у вересні 2022 року, коли відновився саміт «Китай–ЄС» у форматі відеоконференції. Проте тон обговорень змінився. У 2023 році на саміті у Брюсселі ЄС вперше офіційно запропонував «декуплінг» у критичних цифрових технологіях. У спільному комюніке з'явився пункт про «захист стратегічних технологічних активів», що стало кодом для обмеження передачі чутливих технологій [13].

У лютому 2024 року відбулася перша зустріч у новому форматі – «Діалог з питань кібербезпеки та штучного інтелекту», створеному за ініціативою Європейської комісії. Пекін погодився на участь, але відмовився обговорювати питання регулювання ШІ за межами технічних стандартів. У тому ж році ЄС прийняв Закон про штучний інтелект (AI Act), який фактично встановив глобальні стандарти. КНР відреагувала власним «Законом про безпечне використання ШІ» у серпні 2024 року, що свідчило про формування альтернативної нормативної моделі [99].

На саміті у червні 2025 року сторони домовилися про створення «Робочої групи з цифрового суверенітету» – першого формату, де прямо використовувалося це поняття. Однак у комюніке було зафіксовано, що «підходи до цифрового суверенітету залишаються принципово різними» [75]. Діалог тепер носить характер управління конкуренцією, а не побудови спільної архітектури.

Крім того, особливістю політичного діалогу між КНР та ЄС у цифровій сфері є його асиметрична інституційна природа. ЄС, як колективний актор,

намагається говорити єдиним голос, проте на практиці його позиція часто формується під тиском національних інтересів держав-членів. Це створює простір для китайської стратегії «ділення та панування». Наприклад, у 2018–2020 роках КНР активно залучала країни Центральної та Східної Європи через ініціативу «17+1» (з 2023 року – «14+1» після виходу Литви), де цифрові проєкти (зокрема, «розумні міста», кіберінфраструктура) використовувалися як інструмент посилення впливу [20]. У 2019 році спільна заява «17+1» містила положення про «підтримку китайських цифрових рішень», що суперечило єдності ЄС щодо питань безпеки 5G. Це спонукало Європейську комісію у 2021 році фактично демонтувати формат, наголосивши, що «зовнішня політика ЄС не може будуватися на підґрунті субрегіональних ініціатив».

Німеччина та Франція, як лідери ЄС, також демонстрували різні підходи. Німеччина, залежна від експорту промислового обладнання до Китаю, довго виступала проти жорстких обмежень щодо Huawei. Лише у грудні 2022 року Бундестаг прийняв закон, який дозволив частково виключити китайські компоненти з критичної інфраструктури, але з перехідним періодом до 2028 року. Франція, навпаки, ще з 2017 року запровадила обмеження на участь Huawei в своїх 5G-мережах, керуючись принципами «технологічного суверенітету». Ці розбіжності послаблювали позицію ЄС на переговорах із КНР, оскільки Пекін міг апелювати до національних економічних інтересів як до аргументу проти «надмірної регуляції» з боку Брюсселя [44].

Важливим зовнішнім фактором, що вплинув на діалог, була позиція Сполучених Штатів Америки. З приходом до влади адміністрації Дж. Байдена у 2021 році США активізували тиск на союзників щодо відмежування від китайських технологій. У 2022 році було започатковано діалог ЄС–США з питань торгівлі та технологій (Trade and Technology Council, TTC), який фактично став контрвагою китайському впливу [45; 60]. У рамках TTC ЄС та США узгодили підходи до регулювання ШІ, мікроелектроніки та кібербезпеки. Це змусило ЄС переглянути свою позицію щодо КНР: у 2023 році Брюссель відмовився від ідеї «цифрового партнерства» з Пекіном на користь концепції

«обмеженої взаємозалежності». КНР, у свою чергу, сприйняла ТТС як спробу формування технологічного альянсу проти неї, що підсилило риторику «цифрового суверенітету» [58].

Окремо слід зазначити роль міжнародних організацій як альтернативного майданчика цифрового діалогу. КНР та ЄС активно конкурують за вплив у Міжнародному союзі електрозв'язку (ITU), де з 2022 року триває боротьба за стандартизацію 6G. У 2023 році КНР подала рекордну кількість технічних пропозицій з безпеки мереж, тоді як ЄС підтримав ініціативу США щодо «надійних технологічних ланцюгів поставок» [22]. У такому контексті двосторонній діалог між КНР та ЄС часто втрачає значення на користь багатосторонніх форматів, де кожна сторона намагається залучити третіх гравців.

Еволюція політичного діалогу між КНР та ЄС у сфері цифрової співпраці характеризується нерівномірністю: періоди інституційного зближення чергуються з фазами стратегічного охолодження, а формальні домовленості не завжди супроводжуються реалізацією (див. табл. 1.2).

Таблиця 1.2

Хронологія політичного діалогу КНР–ЄС у сфері цифрової співпраці (1995–2025)

Рік	Подія	Контекст / результат
1	2	3
1995	Перша Спільна стратегія «Десятирічний план співпраці між ЄС та Китаєм»	Не містить окремих положень щодо ІТ; цифрова сфера включена в загальну економічну співпрацю.
2000	Перший саміт «Китай–ЄС» (Пекін)	У комюніке згадується співпраця в науці та технологіях, але без деталізації цифрових напрямів.
2003	Спільна декларація «Партнерство на XXI століття»	Вперше згадується «інформаційне суспільство» як напрям співпраці.
2005	Створення Робочої групи з питань інформаційного суспільства в рамках Діалогу з торгівлі та інвестицій	Перший формальний канал для обговорення ІТ-питань на експертному рівні.
2007	Саміт у Пекіні	Домовленість про запуск Діалогу з питань інформаційного суспільства на рівні високопосадовців.
2012	Саміт у Брюсселі	Підписано Спільну заяву про інновації та цифрову економіку; вперше згадуються кібербезпека та

		інтернет-управління.
1	2	3
2015	Запуск Ініціативи з цифрової співпраці КНР–ЄС	Передбачено щорічні зустрічі на рівні заступників міністрів цифрової політики.
2016	Перша зустріч Діалогу з цифрової співпраці (Гуанчжоу, квітень)	Домовленості щодо спільного тестування 5G, обміну досвідом у регулюванні електронної комерції, участь у проєктах Horizon 2020.
2019	Публікація документу ЄС «ЄС–Китай: стратегія зовнішньої політики» (березень)	КНР офіційно названа «економічним конкурентом» і «системним суперником».
2019	Саміт у Брюсселі (квітень)	Перші окремі переговори з кібербезпеки між ENISA та Китайським управлінням з кіберпростору.
2020	Віртуальний Діалог з цифрової економіки (червень)	ЄС висловив занепокоєння щодо участі китайських компаній у 5G-інфраструктурі.
2020	Позиція Ради ЄС під головуванням Німеччини (грудень)	Встановлено механізм перевірки безпеки для вендорів 5G, що фактично обмежує участь Huawei.
2021	Скасування саміту «Китай–ЄС» (квітень)	Реакція на санкції ЄС через ситуацію в Сіньцзяні та контрзаходи КНР; формат високого рівня заморожено.
2022	Відновлення саміту у віртуальному форматі (вересень)	Підтвердження готовності до діалогу, але без конкретних домовленостей у цифровій сфері.
2023	Саміт у Брюсселі (квітень)	У комюніке вперше згадано «захист стратегічних технологічних активів»; ЄС запропонував «декуплінг» у критичних технологіях.
2024	Запуск «Діалогу з питань кібербезпеки та штучного інтелекту» (лютий)	Перша зустріч у новому форматі; КНР відмовилася обговорювати нормативне регулювання ШІ.
2024	Ухвалення ЄС AI Act (березень)	Перший у світі комплексний закон про регулювання ШІ.
2024	Ухвалення КНР «Закону про безпечне використання ШІ» (серпень)	Відповідь на європейський AI Act; зосереджений на національній безпеці та контролі.
2025	Саміт у Брюсселі (червень)	Створено «Робочу групу з цифрового суверенітету»; у комюніке зафіксовано «принципово різні підходи» до цього поняття.

Джерело: складено автором за матеріалами: [3, с. 12]

Наведена хронологія демонструє, що формальні домовленості часто не втілювалися в повноцінні механізми співпраці. Зокрема, участь китайських установ у рамкових програмах ЄС, зокрема Horizon 2020 та на початковому етапі Horizon Europe, обмежувалася переважно технічними напрямами – штучним інтелектом, кібербезпекою та «Інтернетом речей» [51]. Однак уже у 2023 році Європейська комісія ввела обмеження щодо залучення китайських

державних дослідницьких інститутів до проєктів, пов’язаних із чутливими технологіями, що свідчить про перехід від відкритої наукової співпраці до селективного підходу з огляду на ризики національної безпеки [40].

Політичний діалог КНР–ЄС у цифровій сфері пройшов шлях від технічної кооперації до стратегічного суперництва. У 1995–2006 роках цифрові питання були маргінальною темою. У 2007–2018 роках відбувалася інституціалізація діалогу, але в рамках загальної логіки взаємовигідності. Перелом відбувся у 2019–2022 роках, коли цифрова сфера стала полем стратегічного змагання. З 2023 року діалог функціонує в умовах «конкурентного співіснування»: сторони продовжують спілкуватися, щоб уникати ескалації, але не намагаються досягти концептуальної згоди.

Висновки до розділу 1

Отже, поточний стан дослідження встановлює чотири критичні та взаємопов'язані висновки:

По-перше, автори підкреслюють існування стратегічного трикутника США-Китай-ЄС, при цьому Стратегічну автономію ЄС вчені розглядають переважно як залежну змінну, обмежену політикою двох наддержав. Прийняття ЄС більш реалістичної перспективи є прямою відповіддю на посилення структурної конкуренції та зростання матеріальної могутності Китаю.

По-друге, Інформаційно-цифровий вимір міжнародних відносин визначається цифровим суверенітетом та статусом даних як стратегічного ресурсу. КНР і ЄС представляють протилежні моделі: Китай орієнтується на державно-центричний контроль і техноавторитарне управління, тоді як ЄС формує цифровий порядок на базі цінностей, верховенства права та ринкового регулювання. Водночас цифрові технології стають засобом економічного та політичного впливу, а контроль над даними – інструментом стратегічної потуги. Ця дихотомія підкреслює глибокі ідеологічні та політичні відмінності сторін і визначає напрямок конкуренції у цифровому просторі.

По-третє, Європейський Союз та Китайська Народна Республіка стали двома головними, і водночас кардинально різними, архітекторами глобального цифрового порядку. Їхні підходи до цифрової трансформації – це не просто питання економічної політики, а глибоко вкорінені в їхніх відповідних політичних системах та суспільних цінностях.

ЄС прагне до регуляторної моделі, що базується на правах. Його сила полягає в здатності встановлювати високоякісні, юридично обов'язкові правила, які відображають його цінності демократії, основних прав та людиноцентричного підходу до технологій. Ця модель пропонує довіру, правову визначеність та потужний контроль над надмірностями як корпоративної, так і державної влади. Однак її слабкістю є постійний дефіцит промислових масштабів та гнучкості; вона регулює цифровий світ ефективніше, ніж будує його.

Китай удосконалив модель, що базується на суверенітеті та керується державою. Його сила полягає в його здатності до швидкого, масштабного виконання, що підживлюється державним керівництвом та симбіотичними стосунками з його національними лідерами. Ця модель забезпечила вражаюче економічне зростання та технологічний прогрес. Однак його слабкими сторонами є відсутність прозорості, ігнорування прав особистості та конфіденційності, а також модель управління, до якої демократії в усьому світі ставляться з глибокою підозрою.

Загострення конкуренції між цими двома моделями є визначальною геополітичною динамікою цифрової епохи. Вона прискорює фрагментацію інтернету – так званий «розкол інтернету» – де різні регіони світу можуть працювати за принципово різними правилами, технічними стандартами та технологічними екосистемами. Це створює складне та непередбачуване середовище для глобального бізнесу, який повинен орієнтуватися в клаптиковій масі суперечливих регуляторних режимів.

РОЗДІЛ 2. АНАЛІЗ СТАНУ ТА ОСОБЛИВОСТЕЙ ВІДНОСИН КНР ТА ЄС В ІНФОРМАЦІЙНО-ЦИФРОВОМУ ВИМІРІ

2.1. Соціально-політичний та економічний профіль КНР та ЄС як акторів міжнародних відносин

Сучасна міжнародна система характеризується поліархічною конфігурацією влади, у якій на порядок денний виходять не лише традиційні державні актори, а й складні недержавні утворення, здатні впливати на глобальні процеси через економічні, нормативні та технологічні ресурси. Серед таких акторів особливе місце посідають Китайська Народна Республіка та Європейський Союз– суттєво різні за політичною природою, внутрішньою організацією та стратегічними пріоритетами, проте водночас ключові для глобального економічного порядку, геополітичної стабільності та формування нових правил міжнародної взаємодії [25]. Аналіз їхнього соціально-політичного та економічного профілю є необхідною передумовою для розуміння особливостей їхньої участі в міжнародних відносинах, зокрема в контексті зростання конкуренції за вплив у цифровій сфері [36].

Китайська Народна Республіка залишається однією з найбільш централізованих політичних систем сучасності. У 2023 році на XXI з'їзді Комуністичної партії Китаю (КПК) Сі Цзіньпін отримав третій президентський термін, що юридично закріпило його домінування в політичній системі КНР і підтвердило перехід до моделі «персоналізованої влади» [5]. Це посилення вертикалі влади супроводжувалося поглибленням ідеологічного контролю, зокрема через розширення застосування концепції «соціалізму з китайською специфікою епохи Сі Цзіньпіна», яка поєднує економічну відкритість із жорстким політичним авторитаризмом [100].

Демографічна ситуація в КНР у 2025 році є предметом серйозної уваги влади. За даними Державного статистичного управління КНР (National Bureau of Statistics of China), чисельність населення країни становить 1 408,3 млн осіб,

що на 1,2 млн менше, ніж у 2022 році – третій рік поспіль фіксується природне скорочення населення. Середня тривалість життя досягла 78,2 року, а частка осіб у віці 65+ – 15,4%, що свідчить про стрімке старіння суспільства. Ці тенденції створюють значні виклики для уряду: у 2024 році КНР вперше в історії увійшла до фази «демографічного дивіденду від'ємного знаку», коли зменшення працездатного населення починає гальмувати економічний зростання.

Незважаючи на ці виклики, КНР залишається другою за обсягом економікою світу. У 2024 році номінальний ВВП КНР становив 18,3 трлн доларів США (за даними МВФ), що становить близько 14,2% глобального ВВП. Водночас, за паритетом купівельної спроможності (ППС) Китай вже понад десятиліття посідає перше місце у світі. Темпи економічного зростання, хоча й уповільнилися порівняно з попередніми десятиліттями, залишаються відносно високими: у 2024 році – 4,8%, що вище середнього показника для розвинених економік [6]. Основним драйвером росту тепер є внутрішній попит, технологічна модернізація та експорт високотехнологічної продукції.

Глобальна економічна присутність КНР значно посилилася завдяки ініціативі «Один пояс – один шлях» (Belt and Road Initiative, BRI), яка станом на 2025 рік охоплює понад 150 країн і інвестувала понад 1 трлн доларів у інфраструктурні проекти [79]. Однак у 2023–2025 роках КНР поступово трансформує BRI з масштабної інфраструктурної програми в більш вибіркову стратегію «малої, але якісної співпраці», з акцентом на «зелену», цифрову та «здорову» інфраструктуру [4;]. Це свідчить про зміну стратегічного фокусу: від кількісної експансії до якісного впливу [20].

Важливою рисою китайської моделі є тісний зв'язок між державою, партією та економікою. Державні підприємства (ДП) залишаються ключовими гравцями в стратегічних секторах – енергетиці, телекомунікаціях, важкій промисловості. За даними OECD, державні корпорації контролюють понад 60% активів у секторі промисловості. Водночас, через механізми «гібридної влади»

(hybrid authority), держава поширює свій вплив і на приватний сектор – зокрема через партійні комітети в компаніях, таких як Huawei, Alibaba чи Tencent [44].

На противагу централізованій моделі КНР, Європейський Союз є унікальною політичною конструкцією, що поєднує елементи міжурядової співпраці та наднаціонального управління [94]. У 2025 році ЄС нараховує 27 держав-членів з сукупним населенням 444,2 млн осіб (Eurostat, листопад 2025). Середня тривалість життя – 81,4 року, частка населення у віці 65+ – 21,1%, що свідчить про найвищий у світі рівень старіння. Проте, завдяки імміграції, населення ЄС залишається стабільним, хоча неоднорідність демографічних тенденцій між півднем і сходом континенту створює внутрішні напруженості.

Політична система ЄС базується на принципах представницької демократії, верховенства права, захисту прав людини та ринкової економіки. Однак з початку 2010-х років ЄС переживає період «демократичного стресу»: зростання популізму, сепаратистські рухи (наприклад, у Каталонії чи Фландрії), криза біженців, Brexit та російська агресія проти України поставили під сумнів європейську солідарність [11]. Незважаючи на це, ЄС зберігає своє ядро інституцій – Європейську комісію, Раду ЄС, Європейський парламент, Європейський суд – і здатність до колективного ухвалення рішень, хоча й із урахуванням національних інтересів.

Економіка ЄС є найбільшою в світі за обсягом внутрішнього ринку. У 2024 році ВВП ЄС (у номінальному вираженні) становив 19,1 трлн доларів США, що трохи випереджає показник КНР [32]. Однак темпи зростання залишаються скромними – 0,9% у 2024 році (Єврокомісія, жовтень 2025), що пов’язано з енергетичною кризою, інфляцією та геополітичною нестабільністю. Водночас, ЄС залишається лідером за торговим обігом: у 2024 році його частка у світовому експорті товарів становила 14,5% (WTO), а у сфері послуг – 25,3%.

Особливою рисою є регуляторна влада ЄС – здатність формувати глобальні стандарти через внутрішні правила. Це явище, відоме як «брюссельський ефект» або «регуляторний імперіалізм», дозволяє ЄС впливати на поведінку транснаціональних корпорацій навіть за межами своєї юрисдикції

[12]. Прикладами є GDPR у сфері захисту даних, законодавство щодо зеленої трансформації (European Green Deal) або нові правила цифрових ринків (Digital Markets Act) [92].

Проте внутрішня гетерогенність ЄС залишається структурним обмеженням. Розрив між «ядерною Європою» (Німеччина, Франція, Бенілюкс) та периферійними державами, а також відсутність єдиної зовнішньої політики, ускладнюють формування спільної стратегії щодо КНР. Це проявляється, зокрема, у різному ставленні до інвестицій КНР у стратегічну інфраструктуру: тоді як Німеччина захищає економічні зв'язки з Пекіном, країни Центральної Європи (наприклад, Литва, Чехія) демонструють більшу обережність [46].

Порівняльний аналіз показує, що КНР та ЄС є протилежними типами міжнародних акторів (див. табл.1.2). КНР – це унітарна, авторитарна держава з централізованою стратегією та довгостроковим плануванням, де економічна політика є інструментом геополітичного впливу. ЄС – багаторівнева, консенсусна демократія з дифузнішою ідентичністю та реактивним підходом до зовнішніх викликів, де економічна потужність поєднується з нормативним впливом [58].

Таблиця 2.1

Порівняльний соціально-економічний та політичний профіль КНР та ЄС

Показник	Китайська Народна Республіка	Європейський союз
1	2	3
Населення	1 409,7 млн(2023)	448,8 млн(1 січня 2024)
Частка населення 65+	15,4%(2023)	21,3%(2023)
Середня тривалість життя	78,2 року(2023)	81,5 року(2023)
Форма правління	Однопартійна авторитарна республіка (КПК)	Союз парламентських/президентських демократій
Номінальний ВВП (2023)	17,74 трлн дол. США	18,35 трлн дол. США
Номінальний ВВП (2024, оцінка)	18,3 трлн дол. США	19,1 трлн дол. США
Темпи зростання ВВП (2023)	+5,2%	+0,5%
Темпи зростання ВВП (2024, оцінка)	+4,8%	+0,9%
Частка у світовому експорті товарів (2023)	14,2%	14,5%
Основна економічна модель	Державно-капіталістична	Соціальна ринкова економіка +

	(сильний держсектор, стратегічне планування)	єдиний ринок + регуляторна влада
1	2	3
Ключовий інструмент зовнішньої економічної політики	Ініціатива «Один пояс – один шлях» (BRI)	Спільні угоди про вільну торгівлю (наприклад, з Японією, Канадою), Єдиний внутрішній ринок

Джерело: складено автором за матеріалами: [44]

Ця дихотомія визначає їхню взаємодію: доки КНР працює за логікою «реального політичного впливу», ЄС намагається відстоювати «порядок, заснований на правилах». Однак у 2020-х роках спостерігається певна конвергенція: ЄС стає більш прагматичним (наприклад, у питаннях енергетичної безпеки), а КНР активніше використовує нормативні інструменти (наприклад, власну модель цифрового регулювання).

Політична система КНР функціонує на засадах ієрархічної, вертикально інтегрованої влади, де Комуністична партія Китаю (КПК) виступає єдиним джерелом легітимності та стратегічного керівництва. У цій системі державні органи, військові структури, економічні інститути та медіа інтегровані в єдину політичну матрицю, підпорядковану Центральному комітету КПК та його Політбюро [46]. Така модель забезпечує високий рівень стратегічної послідовності та швидкості реалізації політичних рішень, оскільки не потребує узгодження з опозиційними силами або незалежними судовими інституціями. Зокрема, у сфері цифрової політики ця ієрархія дозволяє миттєво перетворювати стратегічні документи, такі як «14-й п’ятирічний план» або «Цифровий Китай», на конкретні адміністративні рішення, нормативні акти та інвестиційні програми.

Ключовим інструментом центрального керівництва є система двоїстого підпорядкування (dual subordination), за якою керівники всіх державних та публічних організацій одночасно підпорядковуються як виконавчій владі, так і партійним комітетам. Ця система поширюється й на приватний сектор – зокрема, з 2016 року партійні комітети обов’язкові у всіх компаніях з понад 100 співробітниками, а в стратегічно важливих підприємствах, таких як Huawei,

Tencent або BYD, партійні структури мають повноваження впливати на стратегічні рішення, зокрема в сфері досліджень і розробок, міжнародної експансії та кадрової політики. Це забезпечує те, що навіть найбільш інноваційні технологічні компанії Китаю залишаються інструментами державної політики, а їхній глобальний вплив функціонально підпорядкований інтересам національної безпеки та ідеологічної стабільності.

З іншого боку, Європейський Союз функціонує як поліцентрна, консенсусна система, де стратегічні рішення вимагають узгодження між незалежними державами-членами, різними інституціями (Комісія, Рада, Парламент) та різноманітними інтересованими сторонами, включаючи громадянське суспільство та бізнес [77]. Ця модель забезпечує високий рівень легітимності, прозорості та захисту прав, але одночасно призводить до повільності у реагуванні на зовнішні виклики. Наприклад, формування єдиної позиції щодо китайських інвестицій у критичну інфраструктуру вимагало понад п’ять років дискусій, під час яких окремі держави, такі як Німеччина чи Угорщина, блокували жорсткіші обмеження через економічні інтереси.

Особливістю ЄС є його наддержавна природа – він не є суверенною державою, але має наднаціональні повноваження у сфері торгівлі, цифрової політики, конкуренції та захисту даних. Це створює парадокс: ЄС може накладати зобов’язання на глобальні цифрові платформи, якщо вони діють на єдиному ринку, але не має прямих повноважень у військовій, фінансовій або міграційній сферах без згоди держав-членів. У результаті Європейська комісія часто виступає як регуляторний глобальний актор, але не як стратегічний гравець зі здатністю до автономної дії в умовах кризи.

Економічно ці різниці трансформуються в два протилежні підходи до ролі держави в ринковій системі. У КНР економічна діяльність – це інструмент досягнення політичних цілей. Державні підприємства (ДП) не лише контролюють ключові сектори, а й активно виконують завдання держави за межами національних кордонів [58]. Наприклад, компанії China Mobile, Huawei чи CRRC діють як «цифрові амбасадори» у рамках ініціативи «Цифровий пояс і

шлях», де закладання оптоволоконних мереж, будівництво дата-центрів або постачання 5G-обладнання поєднується з пропагандою моделі цифрового суверенітету та формуванням технологічної залежності партнерів. У 2024 році державні корпорації КНР становили 78% усіх інвестицій у стратегічну інфраструктуру в країнах Африки та Центральної Азії.

Європейська економічна модель, навпаки, ґрунтується на соціальній ринковій економіці, де держава виступає не як безпосередній учасник ринку, а як регулятор, який забезпечує чесну конкуренцію, захист прав споживачів та екологічну сталість. Приватний сектор, зокрема великі технологічні компанії, функціонує незалежно від держави, а їхня міжнародна активність залежить від ринкової доцільності, а не від політичних завдань [81]. Хоча в останні роки ЄС прагне зміцнити європейських гравців через ініціативи на кшталт European Chips Act або GAIA-X, ці заходи не передбачають прямого державного контролю над компаніями, а лише створення сприятливого екологічного середовища для інвестицій.

Ця різниця відображається й у підходах до стратегічної автономії – поняття, яке стало ключовим для обох акторів у 2020-х роках, але з радикально різним змістом. Для КНР стратегічна автономія означає технологічну незалежність від західних постачальників, досягнуту через державне фінансування, закритість ринку та примусову локалізацію. Програма «Китай – 2025» і «План відродження мікрочипів» є частиною цієї стратегії, спрямованої на створення повного технологічного ланцюга – від сировини до фінальних продуктів.

Для ЄС стратегічна автономія – це нормативна та інституційна незалежність, здатність встановлювати власні правила в цифровому просторі, навіть якщо це означає відмову від співпраці зі стратегічними партнерами. Digital Markets Act, Digital Services Act та AI Act – це не просто регуляторні документи; це спроба ЄС зберегти контроль над цифровою економікою, хоча його власні технологічні гіганти відсутні [11]. Ця модель базується на відкритості для тих, хто дотримується правил, а не на ізоляції.

Важливою характеристикою обох систем є також реакція на кризи. Китайська модель демонструє високу резистентність до шоків завдяки централізованому керівництву та монополії на інформацію. Під час пандемії COVID-19, наприклад, держава швидко мобілізувала ресурси для розвитку цифрових інструментів контролю (health codes, tracking apps), які були інтегровані в систему соціального управління. Однак ця модель має обмежену адаптивну гнучкість – зокрема, у випадку зміни технологічних парадигм (наприклад, переходу на відкриті архітектури ШІ) Китай часто вимушений імітувати іноземні рішення в закритому форматі, що знижує інноваційний потенціал.

ЄС, навпаки, має високу адаптивну здатність завдяки різноманітності думок, відкритості до міжнародної співпраці та гнучкості регуляторних механізмів. Проте його резистентність до шоків обмежена: під час енергетичної кризи 2022–2023 років, наприклад, відсутність єдиного енергетичного ринку та різні підходи держав-членів до постачань із Китаю ускладнювали координацію. Це також стосується цифрової сфери: ЄС швидко реагує на нові виклики (наприклад, регулювання ШІ), але повільно реалізує інфраструктурні проєкти через складність узгодження.

Обидві системи перебувають у стані постійної еволюції. КНР поступово нормативізує свою цифрову політику, приймаючи закони, які формально відповідають міжнародним стандартам (наприклад, Закон про захист особистих даних 2021 року), але зберігають пріоритет держави над особистими правами. ЄС, у свою чергу, стає більш інструменталізованим, використовуючи економічні та регуляторні інструменти для досягнення геополітичних цілей – зокрема, механізм «зниження ризиків» (de-risking) по відношенню до КНР поєднує економічну логіку з безпековими міркуваннями.

Таким чином, соціально-політичний та економічний профіль обох акторів формує не лише їхні внутрішні пріоритети, а й способи участі в міжнародній системі. Саме ці структурні відмінності лягли в основу стратегічного перегляду

відносин у 2019 році і продовжують визначати динаміку їхньої взаємодії в інших сферах, зокрема в інформаційно-цифровому вимірі.

2.2. Аналіз цифрової політики КНР та ЄС у сферах кібербезпеки, штучного інтелекту та цифрового суверенітету

Цифрова політика Китайської Народної Республіки та Європейського Союзу відображає фундаментальні відмінності їхніх політичних систем, економічних моделей та стратегічних пріоритетів. У сфері кібербезпеки, штучного інтелекту та цифрового суверенітету ці розбіжності проявляються найгостріше, формуючи дві конкуруючі парадигми цифрового управління: державно-центричну, суверенітетну модель КНР та ринково-нормативну, правозахисну модель ЄС [25]. Аналіз цих підходів дозволяє зрозуміти не лише внутрішню логіку кожної системи, а й джерела їхнього стратегічного зіткнення на глобальному рівні.

У КНР кібербезпека розглядається як невід'ємна складова національної безпеки. Ключовим документом є Закон про кібербезпеку 2017 року, який встановив обов'язковість локалізації критичних даних на території КНР, вимагає від іноземних компаній передавати вихідні коди програмного забезпечення для перевірки та передбачає створення «системи критичної інформаційної інфраструктури» (СІІО), підпорядкованої державі [66]. У 2021 році закон було доповнено Положенням про кібербезпеку при здійсненні операцій з великими масивами даних, що ввело обов'язковий аудит для компаній, які обробляють дані понад 1 млн користувачів перед виходом на іноземні фондові біржі [81].

Центральним регулятором є Китайське управління з кіберпростору (CAC), створене у 2014 році та підпорядковане Центральній комісії з інтернет-безпеки при Комуністичній партії Китаю. CAC має повноваження блокувати іноземні платформи (зокрема, Google, Facebook, Twitter), вимагати видалення контенту та накладати штрафи у розмірі до 5% від річного обороту компанії. У 2023 році CAC запровадило механізм «кіберпатрулювання» – автоматизовану систему

моніторингу мережі на предмет «антидержавних» чи «психологічно нестабільних» повідомлень [100].

На противагу цьому, ЄС виходить із принципів відкритого Інтернету, захисту приватності та колективної стійкості. Основою кібербезпекової архітектури є Директива NIS2 (2022), яка поширює обов'язки з кібербезпеки на широке коло секторів – від енергетики до хмарних послуг, – і зобов'язує держави-члени створювати національні компетентні органи [72]. Ключовим інститутом на рівні ЄС є Європейське агентство з кібербезпеки (ENISA), яке координує обмін загрозами, сертифікацію продуктів та стрес-тести критичної інфраструктури [21].

Важливим елементом є Загальний регламент з захисту даних (GDPR, 2018), який, хоча й не є документом з кібербезпеки вузько визначеного, фактично став глобальним стандартом захисту даних. GDPR передбачає суворі штрафи за витік даних (до 4% від глобального обороту) та право користувачів на видалення своєї інформації [92]. У 2024 році ЄС запровадив Європейський сертифікат кібербезпеки для IT-продуктів, який поступово стає обов'язковим для виробників, що хочуть вийти на єдиний ринок.

Політика у сфері штучного інтелекту демонструє ще глибші концептуальні розбіжності. У 2024 році ЄС ухвалив Закон про штучний інтелект (AI Act) – перший у світі горизонтальний правовий акт, який класифікує ШІ-системи за рівнем ризику [35]. Заборонено застосування систем соціального рейтингування, певних форм біометричного розпізнавання у публічному просторі та маніпулятивних алгоритмів [49]. Високоризикові системи (у сфері охорони здоров'я, транспорту, освіти) підлягають обов'язковій сертифікації. AI Act базується на принципах людиноцентризму, прозорості та недискримінації.

КНР, навпаки, прагне максимального використання ШІ для економічного зростання та соціального контролю. У 2024 року було прийнято «Закон про безпечне використання штучного інтелекту», який, попри назву, не містить заборон на соціальні рейтинги чи масове розпізнавання облич [17]. Замість цього, він зосереджується на класифікації ШІ-продуктів за рівнем

«національної безпеки» та вимагає від розробників реєструвати великі мовні моделі (LLM) у САС. Алгоритми, що використовуються в державних системах (наприклад, у Сіньцзяні для моніторингу уйгурів), залишаються поза сферою регулювання [100].

Регулювання штучного інтелекту в ЄС та КНР ґрунтується на різних об'єктах контролю. Європейський підхід фокусується на конкретних застосуваннях ШІ: система класифікує рішення за рівнем ризику для фундаментальних прав – забороняє соціальні рейтинги, обмежує використання біометричного розпізнавання в публічному просторі, вимагає аудиту для алгоритмів у сфері працевлаштування чи кредитування [34]. Критерій легітимності – вплив на особу, а не технічна складність моделі.

Китайська стратегія, навпаки, регулює поширення технологій як таких. Закон про безпечне використання ШІ 2024 року встановлює обов'язкову реєстрацію великих мовних моделей у Китайському управлінні з кіберпростору, вимагає фільтрації «неприйнятного» контенту на етапі навчання моделі та забороняє генерацію інформації, що «підриває національну єдність» чи «пропагує небажані цінності» [99]. Цілі моделі, які використовуються всередині державного сектора – наприклад, для прогнозування соціального напруження в Сіньцзяні, – залишаються поза сферою регулювання. Головний критерій – відповідність державній ідеології та інтересам національної безпеки, а не захист прав окремої людини [55].

Поняття «цифрового суверенітету» стало центральним у стратегічному дискурсі обох сторін, але з радикально різним змістом. У ЄС цифровий суверенітет означає здатність країн-членів та громадян контролювати цифрові технології, дані та інфраструктуру без зовнішнього тиску (рис. 2.1) [75].

Розглянемо три взаємопов'язані напрями, які лежать в основі стратегії цифрового суверенітету ЄС. Перший – Європейська хмара Gaia-X – спрямований на створення незалежної від американських (AWS, Azure, Google Cloud) та китайських (Alibaba Cloud, Huawei Cloud) платформ цифрової інфраструктури. Запущена у 2020 році, на початку 2025 року вона об'єднує

понад 300 компаній, державних органів та наукових установ, що свідчить про масштабність інституційного проекту [89].

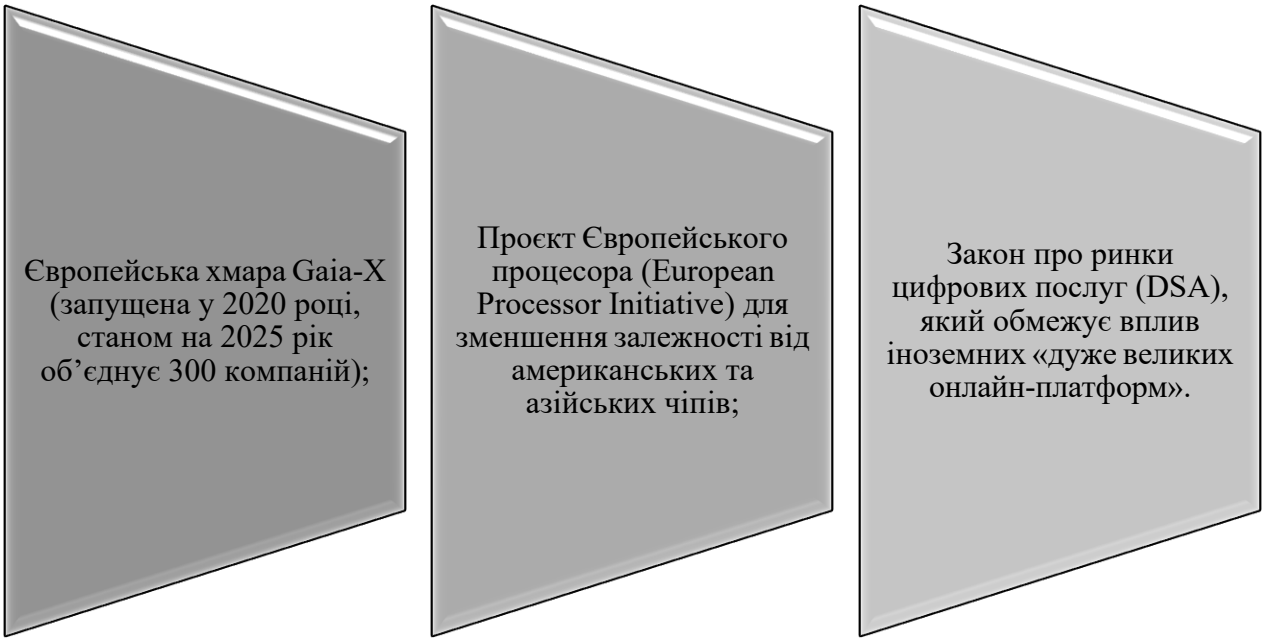

Рис. 2.1. Ключові компоненти цифрового суверенітету ЄС: технологія, регуляція, інфраструктура [89]

Другий – Проєкт Європейського процесора – відповідає за технологічну автономію в сфері мікрочипів, де ЄС залишається залежним від США (Intel, NVIDIA) та Тайваню (TSMC). Цей проєкт має на меті розробку власних архітектур та виробництва чіпів для стратегічних секторів – оборони, енергетики, транспорту [89].

Третій – Закон про ринки цифрових послуг (DSA) – представляє регуляторний інструмент, який дозволяє ЄС встановлювати правила для глобальних платформ, навіть якщо вони не мають фізичного присутності в ЄС. DSA передбачає обмеження на рекламу, алгоритмічну прозорість та механізми скарг, що фактично перетворює ЄС на «регуляторного імперіаліста» у цифровій сфері.

Ці три компоненти разом формують систему, яка дозволяє ЄС зберігати стратегічну автономію без повного відмовлення від глобалізації. На відміну від китайської моделі, яка базується на ізоляції, європейський підхід спирається на

нормативний вплив та технологічну кооперацію з партнерами, що дотримуються європейських стандартів.

Цифровий суверенітет ЄС не передбачає ізоляції. Він спрямований на забезпечення стратегічної автономії – здатності приймати незалежні технологічні та регуляторні рішення в умовах глобальної взаємозалежності. При цьому ЄС залишається відкритим для співпраці з тими партнерами, чиї підходи до захисту даних, кібербезпеки та штучного інтелекту відповідають європейським правовим та етичним стандартам.

У КНР цифровий суверенітет – це доктрина «кіберсуверенітету», сформульована Сі Цзіньпіном ще у 2015 році на світовому інтернет-форумі в Учжень. Вона передбачає повне право кожної держави на незалежне регулювання інтернету на своїй території, без втручання зовнішніх акторів [51]. На практиці це проявляється через ключові механізми, за допомогою яких Китай реалізує концепцію «цифрового суверенітету» (див. рис. 2.2).

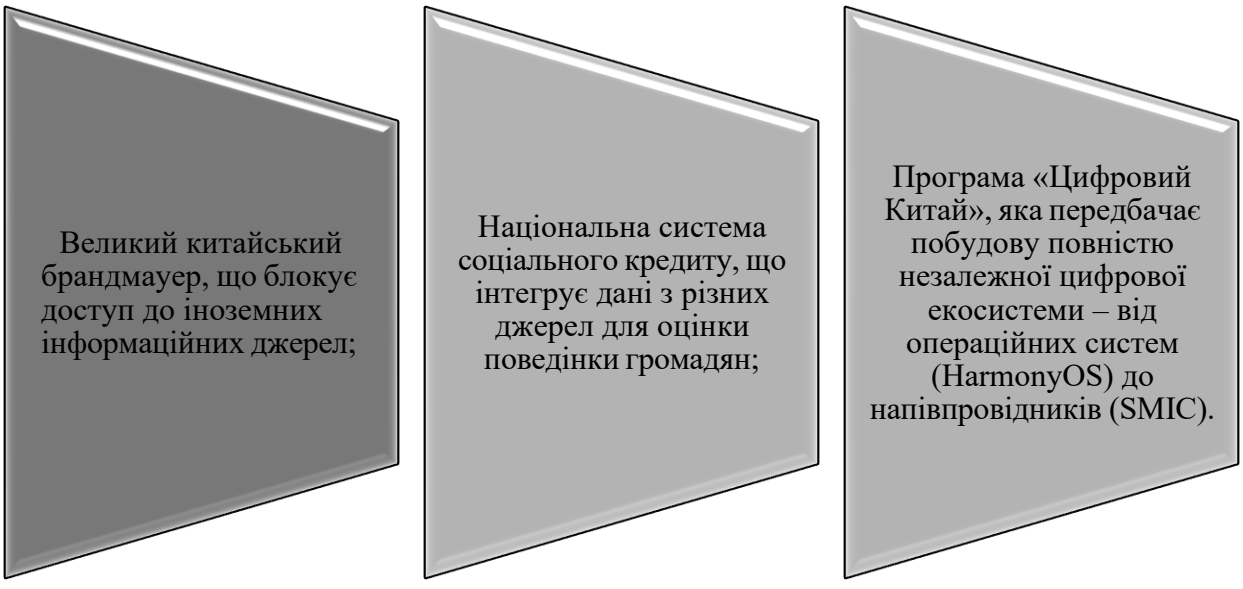

Рис. 2.1. Механізми реалізації цифрового суверенітету в КНР: контроль, моніторинг, автономія [51]

Розглянемо три фундаментальні елементи, що лежать в основі китайської моделі цифрового суверенітету. Перший – Великий китайський брандмауер – є

технічним інструментом, який забезпечує ізоляцію внутрішнього цифрового простору від глобальної мережі. Він блокує доступ до понад 10 тис. іноземних сайтів, включаючи Google, Facebook, Twitter, YouTube, а також платформи, що не проходять перевірку на «соціальне благополуччя» (згідно з Положенням про кібербезпеку 2017 року). Цей механізм дозволяє державі контролювати інформаційний потік та запобігати поширенню «небажаних ідей».

Другий – Національна система соціального кредиту – представляє собою комплексну систему моніторингу поведінки громадян, яка інтегрує дані з банків, поліції, судів, онлайн-платформ та навіть комунальних служб [66]. Система присвоює кожному громадянину рейтинг, який впливає на можливість отримання кредиту, квитків на поїзд, доступу до престижних шкіл чи житла. У 2024 році система була розширена на корпорації, що дозволило державі контролювати не лише поведінку окремих осіб, а й економічні рішення бізнесу.

Третій – Програма «Цифровий Китай» – має на меті створення повністю незалежної цифрової екосистеми. Вона охоплює всі рівні технологічного ланцюга: від операційних систем (HarmonyOS, заміна Android/iOS) до напівпровідників (SMIC, яка виробляє чіпи за 7 нм техпроцесом з 2023 року), обчислювальних хмар (Aliyun, Huawei Cloud) та мобільних мереж (5G/6G за стандартами, розробленими в Китаї) [67]. Це не просто економічна стратегія – це ідеологічний проект, спрямований на формування «цифрової цивілізації з китайською специфікою».

Ці три компоненти разом утворюють замкнену систему цифрового контролю, де держава є єдиним арбітром інформації, поведінки та технологічного розвитку. На відміну від ЄС, який намагається збалансувати відкритість та безпеку, КНР вибирає абсолютний контроль як умову стабільності [68]. Ця модель не передбачає компромісів з глобальними нормами – вона спирається на принцип «суверенітету над інтернетом», який не допускає зовнішнього втручання ні в технічну, ні в правову, ні в етичну сферу.

Важливо звернути увагу на те, що ключова відмінність полягає в об’єкті захисту. Європейський цифровий суверенітет спрямований на захист особистих

прав і свобод: GDPR гарантує контроль над власними даними, AI Act забороняє соціальні рейтинги та непрозорі алгоритми маніпуляції, а DSA зобов'язує платформи пояснювати, як формується контент. У цій моделі технології підпорядковані індивіду – громадянин має право на вибір, прозорість і оскарження автоматизованих рішень.

Китайський цифровий суверенітет, навпаки, орієнтований на захист держави від будь-якого зовнішнього впливу та внутрішньої нестабільності. Великий брандмауер ізольовує китайський інтернет від глобальних інформаційних потоків. Система соціального кредиту інтегрує дані з різних джерел для оцінки лояльності громадянина. Закон про кібербезпеку зобов'язує компанії передавати дані державі без судового рішення [69]. Тут особистий вибір поступається стратегічній меті – підтриманню політичної стабільності через технологічний контроль.

Порівняння цифрової політики Китайської Народної Республіки та Європейського Союзу розкриває різницю у регуляторних механізмах й фундаментальну дивергенцію у концептуальних підходах до ролі технологій у суспільному та політичному житті. Ця дивергенція проявляється у різних інституційних архітектурах, що управляють кіберпростором, різних цілях регулювання штучного інтелекту та різних трактуваннях поняття цифрового суверенітету [70]. Важливо підкреслити, що ці підходи не є випадковими чи тактичними – вони укорінені в політичних системах, ідеологічних парадигмах та історичному досвіді обох акторів.

У КНР цифрова політика є продовженням державної стратегії забезпечення внутрішньої стабільності та технологічної автономії. Кібербезпека розглядається не як технічна проблема, а як питання національної безпеки, де будь-яке зовнішнє втручання в інформаційні процеси сприймається як потенційна загроза суверенітету. Закон про кібербезпеку 2017 року, а також подальші нормативні акти, створили юридичну базу для повного контролю над цифровим простором. Ключовим елементом цієї системи є обов'язкова локалізація даних, що дозволяє державі мати прямий доступ до інформаційних

потоків. Важливим інструментом цього контролю є Китайське управління з кіберпростору (CAC), яке виконує не лише регуляторні, а й цензорські функції. Наприклад, у 2023 році CAC запровадило систему автоматизованого моніторингу, яка виявляє та блокує контент, що, на думку влади, може загрожувати соціальній гармонії [72]. Такий підхід гарантує, що цифровий простір стає інструментом управління суспільною думкою, а не каналом для вільного обміну ідеями.

У сфері штучного інтелекту КНР дотримується аналогічної логіки. Технології ШІ інтегровані в державну систему управління, зокрема через проєкти, пов'язані з прогнозуванням соціального напруження, моніторингом етнічних меншин та автоматизацією адміністративних процесів. «Закон про безпечне використання штучного інтелекту» 2024 року не став винятком – навпаки, він юридично закріпив пріоритет державних інтересів над індивідуальними правами. Зокрема, він вимагає від розробників реєструвати великі мовні моделі (LLM) та впроваджувати механізми фільтрації вмісту, який може «підривати національну єдність» [81]. При цьому державні системи, що використовують ШІ для внутрішнього контролю (наприклад, у Сіньцзян-Уйгурському автономному районі), залишаються поза полем регулювання. Це свідчить про те, що регуляція в КНР не має на меті захист прав громадян, а зосереджена на запобіганні технологічному використанню, яке суперечить офіційній ідеології.

Європейський Союз, навпаки, будує свою цифрову політику навколо принципів прав людини, верховенства права та відкритої конкуренції. Кібербезпека в ЄС розглядається як колективне завдання, до вирішення якого залучаються як державні, так і приватні актори. Директива NIS2 (2022) поширює обов'язки щодо кіберзахисту на критичні сектори економіки, а Європейське агентство з кібербезпеки (ENISA) виступає координувальним органом, який забезпечує обмін інформацією про загрози та гармонізацію стандартів. Паралельно з кібербезпекою, ЄС активно розробляє політику захисту персональних даних. Загальний регламент з захисту даних (GDPR) став

глобальним еталоном у цій сфері, встановлюючи чіткі права користувачів і суворі санкції за їхнє порушення. У 2024 році до цієї системи додався Європейський сертифікат кібербезпеки, що вимагає від виробників IT-продукції підтвердження відповідності визначеним критеріям безпеки.

Щодо штучного інтелекту, ЄС прагне встановити етичні та правові рамки, які обмежують застосування технологій у чутливих сферах. AI Act 2024 року – перший у світі комплексний законодавчий акт щодо ШІ – вводить ризик-орієнтований підхід: найбільш небезпечні застосування (соціальне рейтингування, біометричне розпізнавання у загальнодоступних місцях) заборонені, тоді як високоризикові системи (у сфері охорони здоров'я, транспорту, освіти) потребують обов'язкової сертифікації [82]. Цей підхід відображає фундаментальне переконання: технології повинні бути підконтрольні людині, а не навпаки. Прозорість, відповідальність розробників та можливість оскарження автоматизованих рішень є ключовими елементами цієї моделі.

Поняття цифрового суверенітету в обох системах виконує різні функції. У ЄС воно вказує на здатність діяти незалежно в глобальному цифровому середовищі, не втрачаючи при цьому відкритості. Проєкти на зразок Gaia-X, Європейського процесора та законодавчі ініціативи, такі як DSA та DMA, спрямовані на створення альтернативної технологічної бази, яка дозволить ЄС зберігати контроль над власними даними та критичною інфраструктурою. У КНР цифровий суверенітет реалізується через повну ізоляцію: Великий китайський брандмауер, Національна система соціального кредиту, програма «Цифровий Китай» – усе це формує замкнену екосистему, де держава контролює кожен елемент технологічного ланцюга [71]. У цій системі відкритість сприймається як загроза, а регулювання – як засіб недопущення зовнішнього впливу.

Цифрова політика КНР та ЄС відображає дві альтернативні моделі організації цифрового простору. ЄС будують регульований, відкритий, правозахисний простір, де технології повинні служити людині. КНР створює

державно-контрольований, закритий, безпечний для режиму простір, де технології є інструментом стабільності та ефективності. Ці моделі не просто різняться – вони несумісні на концептуальному рівні, що пояснює, чому навіть технічна співпраця між ними обмежується вузькими сферами, а політичний діалог не веде до конвергенції стандартів.

2.3. Механізми та інструменти інформаційно-цифрової взаємодії між КНР і ЄС

Інформаційно-цифрова взаємодія між Китайською Народною Республікою та Європейським Союзом реалізується через сукупність формальних та неформальних механізмів, які діють паралельно з політичним діалогом та незалежно від внутрішніх цифрових політик сторін. Ці механізми охоплюють інституційні платформи, технічні проєкти, регуляторні процеси та конфліктні інструменти. Вони відображають складну динаміку, у якій елементи співпраці, конкуренції та конфронтації існують одночасно.

Найвищим рівнем інституційної взаємодії залишається Діалог з питань цифрової економіки КНР–ЄС, започаткований у 2015 році та відновлений у 2022 році після перерви. Формат передбачає щорічні зустрічі на рівні заступників міністрів цифрової політики та керівників профільних агентств. Однак після 2023 року його мандат було звужено: зустрічі тепер фокусуються лише на технічних питаннях – сумісності стандартів у сфері «Інтернету речей», енергоефективності дата-центрів, класифікації даних [31]. Стратегічні теми – кібербезпека, ШІ, цифровий суверенітет – винесені в окремі формати.

У лютому 2024 року було створено Діалог з питань кібербезпеки та штучного інтелекту, який проводиться раз на півроку. Перша зустріч у Берліні (лютий 2024) обмежилася обміном поглядами щодо визначення «надійного ШІ»; друга (Пекін, вересень 2024) – обговоренням критеріїв для включення компаній до «списків довіри» у кіберпросторі. Проте жодна зі сторін не погодилася на взаємне визнання своїх сертифікаційних систем. У червні 2025 року на саміті КНР–ЄС було домовлено про створення Робочої групи з

цифрового суверенітету, яка працює на експертному рівні. На сьогодні її основне завдання – узгодження термінології, оскільки сторони не можуть знайти спільного розуміння навіть щодо базових понять [61].

Окрім цього, у рамках Спільного науково-технічного комітету КНР–ЄС (заснований у 2004) діє підкомітет з цифрових технологій, який координує участь китайських установ у проєктах Horizon Europe. Станом на 2025 рік китайські університети та дослідницькі центри беруть участь у 17 проєктах Horizon Europe у сферах квантових обчислень, мікроелектроніки та «зелених» ІТ-рішень [79]. Однак усі проєкти підлягають попередній перевірці на наявність чутливих технологій, а доступ до даних обмежено.

Найбільш продуктивною, хоча й обмеженою за масштабами, сферою фактичної інформаційно-цифрової взаємодії між КНР та ЄС залишається фундаментальна наука та прикладна інженерія, де взаємодоповнюваність дослідницьких компетенцій ще здатна переважати над стратегічною недовірою. Найяскравішим прикладом була співпраця у сфері мобільних мереж п’ятого та шостого поколінь. У рамках європейської ініціативи 5G Public-Private Partnership (5G-PPP), фінансованої з програми Horizon 2020, компанії Huawei та Ericsson протягом 2018–2021 років брали участь у спільних технічних випробуваннях сумісності між різними архітектурами 5G-мереж [3]. Ці дослідження мали на меті гармонізацію протоколів, зменшення інтерференції між базовими станціями та оптимізацію використання радіочастотного спектру. Однак після 2022 року, на тлі посилення політичного тиску з боку США та прийняття ЄС Стратегії економічної безпеки, Huawei була фактично виключена з усіх європейських тестових мереж [66]. Незважаючи на це, технічна взаємодія не припинилася повністю: на рівні дослідницьких лабораторій продовжується обмін результатами моделювання радіохвиль. Зокрема, у Institut Mines-Télécom (Франція) та Fraunhofer Society (Німеччина) діють спільні групи з китайськими колегами з Університету Цінхуа та Шанхайського інституту мікроелектроніки, які працюють над стандартами 6G у частині використання високочастотного діапазону (від 24 до 100 ГГц) [22].

У сфері штучного інтелекту найважливішим проєктом став AICODE (Artificial Intelligence for Cross-border Open Data Environments), запущений у 2020 році в рамках Horizon 2020. У ньому брали участь Університет Цінхуа (Пекін), Сорбонна (Париж), Технічний університет Мюнхена, а також компанії DeepTech EU та SenseTime. Основною метою проєкту було розроблення методів ананімізації даних для безпечного трансграничного обміну інформацією в наукових дослідженнях [98]. Проте вже у 2021 році Європейська комісія ввела додаткові обмеження на передачу даних до країн, де діють закони, що зобов'язують компанії передавати інформацію державі без судового рішення. Це зробило співпрацю з КНР технічно неможливою в рамках європейського законодавства. Проєкт завершився у 2022 році без продовження, хоча його результати (пакети алгоритмів диференційної приватності) залишилися відкритими для наукового співтовариства.

У сфері кібербезпеки формальна співпраця обмежувалася двостороннім обміном досвідом між Європейським агентством з кібербезпеки (ENISA) та Китайським центром з кібербезпеки (China Cybersecurity Center, CCSC) протягом 2021–2023 років. Сторони спільно розробляли методології реагування на масштабні DDoS-атаки на критичну інфраструктуру – енергосистеми, транспортні мережі, державні реєстри [72]. Основна увага приділялася синхронізації протоколів сповіщення про інциденти та автоматизованого блокування зловмисного трафіку. Однак у 2023 році ЄС запропонував створити спільну базу даних про джерела кібератак. Китайська сторона відмовилася, посилаючись на національне законодавство, яке забороняє вивіз даних про кіберінциденти за межі КНР. Після цього проєкт припинив існування. На сьогодні жодних офіційних каналів технічної взаємодії між ENISA та китайськими органами кібербезпеки не існує.

Важливо звернути увагу, що навіть у тих сферах, де співпраця продовжується, вона функціонує в умовах постійного регуляторного тиску, обмежень на обмін даними та відсутності довіри на інституційному рівні. Фактична взаємодія зводиться до мінімально можливого рівня, достатнього

лише для підтримки наукового діалогу, але недостатнього для формування спільних технологічних рішень.

Крім того, важливим каналом залишаються міжуніверситетські угоди. Станом на 2025 рік існує понад 120 угод між європейськими та китайськими вишами у сфері комп'ютерних наук. Найактивніші – Університет Цінхуа, Чжечжянський університет, Сорбонна, Кембридж, Технічний університет Делфт [51].

Однією з форм інформаційно-цифрової взаємодії є конкуренція в сфері нормотворчості. ЄС та КНР одночасно виступають ініціаторами альтернативних технічних стандартів:

У Міжнародному союзі електрозв'язку (ITU) КНР просуває стандарти безпеки 6G, які передбачають інтеграцію «національних модулів автентифікації» [93]. ЄС підтримує альтернативну пропозицію, засновану на відкритих протоколах.

1. У Міжнародній організації зі стандартизації (ISO) триває боротьба за ухвалення стандарту щодо етики ШІ. Пропозиція КНР робить акцент на «соціальній гармонії», версія ЄС – на «правах людини» [99]. Станом на листопад 2025 року компроміс не досягнуто.

2. У сфері кібербезпеки КНР запропонувала у ООН резолюцію «Про суверенітет у кіберпросторі», яку підтримали понад 70 країн. ЄС, разом із США та союзниками, запропонував альтернативну ініціативу «Правила цифрового поведінки», що ґрунтується на міжнародному праві та правах людини [81]. Ці ініціативи конкурують у рамках Робочої групи ООН з кібербезпеки.

Ця «війна стандартів» є формою непрямої взаємодії, де кожна сторона намагається встановити глобальні правила, які відповідають її внутрішній моделі.

Через відсутність ефективних кооперативних механізмів у стратегічних сферах обидві сторони все частіше застосовують інструменти економічної безпеки:

ЄС запровадив механізм перевірки інвестицій (2019), який дозволяє блокувати закупівлю критичної інфраструктури іноземними компаніями. Станом на 2025 рік 14 китайських інвестицій у сфері дата-центрів та оптоволоконних мереж були заблоковані [40].

З 2023 року інформаційно-цифрова взаємодія між КНР та ЄС все частіше реалізується не через кооперацію, а через застосування інструментів економічної безпеки, що мають прямо чи опосередковано цифровий вимір. У жовтні 2023 року Європейська комісія офіційно запустила антисубсидійне розслідування щодо імпорту електромобілів з КНР, підозрюючи, що китайські виробники (зокрема, BYD, NIO та Geely) отримують державну підтримку, яка дозволяє їм пропонувати продукцію за цінами нижче витрат [27; 32]. Проте вже у квітні 2024 року межі розслідування були розширені: у фокус увійшли не лише транспортні засоби як такі, а й їхні вмонтовані цифрові компоненти – бортові комп'ютери, сенсорні системи, модулі штучного інтелекту для навігації та управління. Це стало першим випадком, коли антисубсидійний механізм ЄС було застосовано не лише до промислового виробництва, а й до інтегрованих цифрових технологій. Очікується, що остаточне рішення, яке може призвести до введення мит у розмірі до 25%, буде ухвалене у першому кварталі 2026 року.

У відповідь КНР активізувала власні інструменти економічного тиску. З серпня 2023 року Китай ввів ліцензування експорту 17 рідкісноземельних елементів, зокрема галію, германію та неодиму, які є критичними для виробництва напівпровідників, лазерів, магнітів та оптоволоконних систем [37; 70]. Хоча офіційно ці обмеження мотивувалися «потребами національної безпеки» та не мали прямої адресації на ЄС, їхні наслідки були відчутні вже у перші місяці. Наприклад, франко-італійська компанія STMicroelectronics, один із лідерів європейського напівпровідникового сектора, повідомила про затримки в постачанні сировини для виробництва чіпів, використовуваних у автомобільній електроніці та промислових датчиках. Подібні кроки демонструють, що обидві сторони все частіше використовують цифрові технології як зброю у глобальному економічному суперництві, де обмеження

поставок стратегічних матеріалів або введення митних бар'єрів стають заміною для прямих дипломатичних конфліктів.

Оскільки двосторонні інституційні механізми втрачають ефективність, КНР та ЄС все більше звертаються до багатосторонніх форматів, щоб посилити свій вплив та залучити третіх гравців. Незважаючи на офіційну позицію Європейської комісії, яка у 2021 році оголосила про демонтаж ініціативи «17+1» через її несумісність із принципом єдності ЄС, країни Центральної та Східної Європи продовжують брати участь у цифрових проєктах з КНР на двосторонній основі [20]. Так, у 2024–2025 роках у Польщі (м. Варшава), Словаччині (м. Братислава) та Угорщині (м. Будапешт) запущено пілотні проєкти «розумних міст» за участю китайських компаній Huawei та ZTE, які постачають інфраструктуру для інтегрованого моніторингу транспорту, енергоспоживання та комунальних послуг [24]. Ці проєкти формально фінансуються національними бюджетами, але часто супроводжуються кредитами з Китайського банку експорту та імпорту.

На глобальному рівні важливим майданчиком непрямого діалогу залишається Глобальний форум з цифрової співпраці (Global Forum on Digital Cooperation), створений за ініціативою Генерального секретаря ООН у 2019 році [69]. Незважаючи на те, що КНР та ЄС подають у ньому принципово різні пропозиції – Пекін наголошує на «суверенітеті даних», Брюссель – на «правах людини в цифровому просторі», – обидві сторони беруть участь у спільних робочих групах з цифрової ідентифікації, кіберосвіти та захисту дітей у мережі. Це дозволяє їм підтримувати мінімальний рівень взаємодії без політичних зобов'язань.

Найбільш показовим, однак, є формування конкуруючих ланцюгів поставок у напівпровідниковій сфері. У травні 2024 року ЄС, США, Японія та Республіка Корея ухвалили Брюссельську декларацію про надійні напівпровідникові ланцюги, яка передбачає координацію інвестицій, гармонізацію стандартів безпеки та створення «клубу надійних постачальників». У відповідь КНР у грудні 2024 року започаткувала Азійський

альянс з цифрової автономії, до якого увійшли Китай, Росія, Іран та, частково, Південна Корея (через неформальну участь в окремих проєктах). Цей альянс спрямований на створення альтернативної екосистеми – від виробництва кремнію до розробки власних операційних систем [77]. Таким чином, інформаційно-цифрова взаємодія між КНР та ЄС поступово трансформується з двостороннього діалогу на процес формування двополюсного цифрового світу, де кожен полюс прагне зробити інший стратегічно незначним через створення автономних технологічних ланцюгів, нормативних систем і геополітичних коаліцій.

Характер інформаційно-цифрової взаємодії між Китайською Народною Республікою та Європейським Союзом на початку другої чверті XXI століття визначається не стільки наявністю спільних інтересів, скільки структурною несумісністю їхніх внутрішніх моделей організації цифрового простору. Ця несумісність проявляється у різних підходах до визначення безпеки, відповідальності, прозорості та ролі держави, що призводить до інституціонального розриву в усіх форматах двосторонньої взаємодії [78]. Однак, попри цю фундаментальну розбіжність, повне розмежування залишається неможливим через глобальну взаємозалежність технологічних ланцюгів поставок, наукових досліджень та інфраструктурних систем. Тому замість конфронтації виникає новий режим – режим регульованого конфлікту, у якому взаємодія здійснюється через механізми, що дозволяють уникати прямих зіткнень, зберігаючи при цьому технічну мінімальну взаємодію.

Особливу роль у цьому контексті відіграють міжнародні організації стандартизації, які стають ареною нормативної конкуренції. Міжнародний союз електрозв’язку (ITU), Міжнародна організація зі стандартизації (ISO) та Інститут інженерів з електротехніки та електроніки (IEEE) перетворюються на майданчики, де відбувається бій за формування глобальних технічних норм. Китайська Народна Республіка активно використовує свої фінансові та дипломатичні ресурси для просування власних підходів [79]. Зокрема, у рамках ITU китайські експерти просувають концепцію «національних модулів

автентифікації» у стандартах 6G, які фактично закладають можливість державного контролю над криптографічними ключами. З боку ЄС такі пропозиції сприймаються як загроза цілісності відкритого Інтернету та безпеці критичної інфраструктури [80]. У відповідь Європейська комісія координує позицію з США, Японією та Південною Кореєю, пропонуючи альтернативні стандарти, засновані на принципах end-to-end шифрування та незалежного аудиту.

Подібний підхід спостерігається й у сфері штучного інтелекту. У рамках технічного комітету ISO/IEC JTC 1/SC 42, що займається стандартизацією ШІ, китайська делегація настоює на включенні поняття «соціальної стабільності» як ключового критерію оцінки надійності алгоритмів. У свою чергу, європейські експерти наполягають на закріпленні у стандартах норм AI Act, зокрема заборони соціального рейтингування та обов'язкової сертифікації високоризикових систем [81]. Станом на 2025 рік компроміс не досягнуто, що свідчить про принципову неможливість уніфікації нормативних підходів. Як наслідок, глобальні компанії змушені підтримувати дві окремі версії продуктів – одну для ринків, орієнтованих на європейські стандарти, іншу – для країн, що приймають китайську модель.

Окрім нормативної конкуренції, важливою формою взаємодії залишається технічна співпраця у рамках академічних інституцій. Незважаючи на обмеження з боку Європейської комісії щодо участі китайських державних дослідницьких центрів у проєктах Horizon Europe, науковці обох сторін продовжують підтримувати контакти через двосторонні угоди між університетами. Найбільш активні зв'язки існують між Університетом Цінхуа та вишами Франції, Німеччини та Нідерландів [82]. Ці контакти здебільшого обмежуються обміном публікаціями, участь у конференціях та спільними публікаціями у наукових журналах з високим імпакт-фактором. Важливо, що такі формати взаємодії не передбачають передачі чутливих технологій чи персональних даних, що дозволяє уникати регуляторних ризиків. Разом з тим,

саме ці контакти стають важливим каналом для збереження базового рівня довіри та взаєморозуміння на експертному рівні.

Технологічні проєкти, що реалізуються на місцевому рівні, також формують окремий шар інформаційно-цифрової взаємодії. Міста ЄС та КНР продовжують брати участь у спільних ініціативах у сфері «розумних міст», незважаючи на політичні ризики. У цьому контексті важливу роль відіграють міжнародні міські мережі, такі як C40 Cities або ICLEI, які фокусуються на екологічних та інфраструктурних питаннях, уникнувши при цьому чутливих тем кібербезпеки чи державного контролю [84]. Проєкти з обміну даними щодо управління транспортними потоками чи моніторингу якості повітря реалізуються за умови анонімізації інформації та локалізації даних. Такий підхід дозволяє містам отримувати практичну користь від обміну досвідом, не вступаючи в конфлікт із національним регулюванням.

Слід окремо зазначити роль тіньових каналів, через які китайські компанії отримують доступ до заборонених технологій та програмного забезпечення. Ці канали функціонують через треті країни, які не є учасниками режимів експортного контролю, таких як Вассенаарська угода. Наприклад, Малайзія та В’єтнам стали ключовими вузлами у постачанні обладнання для проектування мікросхем (EDA-програм) та готових чіпів. Механізм діє за схемою: американське чи європейське програмне забезпечення закуповується локальними стартапами в регіоні Південно-Східної Азії, які формально використовують його для внутрішніх потреб, але насправді надають доступ китайським інженерам через хмарні сесії. Ця практика дозволяє китайським компаніям обходити прямі обмеження, хоча й зі значними фінансовими витратами [85]. Для ЄС це створює нові виклики у сфері контролю за дотриманням санкційних режимів, оскільки традиційні механізми митного регулювання виявляються недостатніми.

Економічні інструменти стали ще однією формою взаємодії, що замінює прямий діалог. Антисубсидійні розслідування ЄС щодо китайських електромобілів, розширені у 2024 році на цифрові компоненти, демонструють

новий тренд – інтеграцію цифрової політики в інструментарій торгової оборони. Це свідчить про те, що цифрові технології більше не розглядаються як окрема сфера, а як невід'ємна частина індустріальної та економічної стратегії. Китай, у свою чергу, використовує контроль над рідкісноземельними елементами як важіль тиску у відповідь на такі заходи [63]. Ліцензування експорту галію та германію, введено у серпні 2023 року, прямо вплинуло на виробництво напівпровідників у Європі, зокрема на компанії STMicroelectronics та Infineon. Ця взаємна залежність перетворюється на поле для «тихої війни», де кожна сторона намагається створити стратегічні переваги без ескалації до відкритої конфронтації.

У контексті багатосторонньої дипломатії помітним є зростання ролі Глобального форуму з цифрової співпраці при ООН. Незважаючи на фундаментальні розбіжності, обидві сторони беруть участь у робочих групах з цифрової ідентичності, кіберосвіти та захисту дітей у мережі. Ці напрями обрано не випадково: вони не торкаються стратегічних питань суверенітету чи безпеки, але дозволяють зберігати формальний канал взаємодії [77]. Це також створює можливість для спільних ініціатив у третіх країнах. Наприклад, проєкт «Цифрове підприємництво для МСП у Африці» об'єднує європейські методології та китайську інфраструктуру для підтримки місцевих підприємців. Такі ініціативи, хоча й не мають глобального впливу, демонструють можливість сегментованої співпраці на користь третіх сторін.

Формування альтернативних ланцюгів поставок у напівпровідниковій сфері також є показником переходу до моделі структурованої конкуренції. Брюссельська декларація 2024 року, підписана ЄС, США, Японією та Республікою Корея, закладає основи «клубу надійних постачальників», який має забезпечити захищеність ланцюгів поставок від авторитарних впливів. У відповідь КНР ініціювала створення Азійського альянсу з цифрової автономії, до якого увійшли Китай, Росія, Іран та низка країн Азії [32]. Цей альянс спрямований на створення замкненої екосистеми – від виробництва полікремнію до розробки власних операційних систем. Такий підхід свідчить

про те, що глобальний цифровий простір поступово фрагментується на окремі технологічні блоки, кожен із яких базується на власній ідеологічній та нормативній основі.

Разом з тим, повна ізоляція між цими блоками залишається малоймовірною через економічну доцільність і наукову необхідність. Тому ключовим завданням для обох сторін стає розробка механізмів «безпечного контакту» – форматів взаємодії, які забезпечують обмін знаннями та технологіями без загрози для безпеки чи суверенітету [71]. Такі механізми вже почали формуватися у вузьких сферах, таких як енергоефективність дата-центрів, кібергігієна для малого бізнесу чи етичні аспекти штучного інтелекту. Ці сфери обрано навмисно: вони не мають прямого зв’язку з національною безпекою, але мають практичну цінність для обох сторін.

Інформаційно-цифрова взаємодія між КНР та ЄС переходить у нову фазу, де головним принципом стає не довіра, а взаємне стримування. Обидві сторони усвідомлюють, що повна конвергенція їхніх моделей неможлива, але також розуміють, що повне розмежування неможливе. Тому замість спроб досягнення стратегічної згоди формується новий режим управління розколом – через технічну кооперацію у безпечних нішах, нормативну конкуренцію в міжнародних організаціях та економічні інструменти як еквівалент політичного тиску [70]. Ця модель не гарантує стабільності, але дозволяє уникати ескалації, зберігаючи мінімальний рівень взаємодії, необхідний для функціонування глобальної цифрової економіки.

Одним із ключових наслідків цього підходу є трансформація ролі технологічних компаній. Якщо раніше вони були лише виконавцями державної політики, то сьогодні вони стають носіями технічної автономії, яка дозволяє зберігати міжсистемні зв’язки навіть за умов політичного розриву. Компанії, такі як Huawei, Ericsson, Siemens чи STMicroelectronics, змушені розробляти дуальні стратегії – вони повинні відповідати вимогам європейського регулювання та адаптуватися до китайської моделі. Це призводить до зростання витрат, але також створює нові можливості для інновацій, спрямованих на

універсальність рішень [80]. У цьому контексті компанії перетворюються на ключових акторів цифрової дипломатії, їхні рішення часто визначають напрямок глобального технічного розвитку більше, ніж формальні міждержавні угоди.

Отже, механізми інформаційно-цифрової взаємодії між КНР та ЄС на 2025 рік характеризуються фрагментацією та дуалізмом. Там, де ще можлива технічна кооперація (наука, інженерія), вона жорстко обмежена. У стратегічних сферах (кібербезпека, ШІ, напівпровідники) домінує конкуренція через стандарти, регуляцію та економічні інструменти. Двосторонні формати втратили стратегічний зміст і перетворилися на канали управління конфліктом. Фактична взаємодія тепер відбувається більше в багатосторонніх організаціях, де кожна сторона намагається залучити третіх гравців на свій бік. Це свідчить про те, що відносини КНР–ЄС у цифровій сфері переходить у фазу структурованої конкуренції, де співіснування забезпечується не через взаємне довіру, а через взаємне стримування.

Висновки до розділу 2

Провівши аналіз стану та особливостей відносин Китайської Народної Республіки та Європейського Союзу в інформаційно-цифровому вимірі, можна зробити наступні висновки.

По-перше, політичний діалог у цифровій сфері пройшов чітку еволюцію від технічної кооперації до стратегічного змагання. Якщо в 1995–2018 роках домінував прагматичний підхід, заснований на взаємній економічній вигоді, то після 2019 року, у зв’язку зі стратегічним переосмисленням ЄС щодо КНР, діалог став інструментом управління конкуренцією. На сьогодні він функціонує в умовах «конкурентного співіснування», де формальні зустрічі мають на меті уникнення ескалації, а не досягнення концептуальної згоди.

По-друге, внутрішні цифрові політики КНР та ЄС базуються на фундаментально різних ціннісних основах. ЄС будує регульований, відкритий і правозахисний цифровий простір, де технології підпорядковані особистим

правам і вибору громадян. КНР, навпаки, формує державно-контрольований, закритий і безпечний для режиму простір, у якому технології слугують інструментом соціального контролю та національної стабільності. Ці моделі не лише відрізняються – вони несумісні на концептуальному рівні, що робить конвергенцію стандартів малоймовірною навіть у довгостроковій перспективі.

По-третє, фактичні механізми інформаційно-цифрової взаємодії між КНР та ЄС характеризуються фрагментацією. Там, де ще можлива співпраця (фундаментальні дослідження, інженерія), вона жорстко обмежена регуляторними бар'єрами. У стратегічних сферах (кібербезпека, ШІ, напівпровідники) взаємодія здійснюється переважно через конкуренцію за стандарти, застосування інструментів економічної безпеки та формування паралельних технологічних екосистем. Двосторонні формати втратили стратегічну значущість і перетворилися на канали технічного обміну мінімального рівня.

Таким чином, інформаційно-цифровий вимір є одним із найгостріших і найбільш структурних напрямів сучасних відносин між Китайською Народною Республікою та Європейським Союзом. У цій сфері зіштовхуються не просто різні технологічні підходи чи регуляторні моделі, а фундаментально протилежні уявлення про організацію цифрового суспільства. Для ЄС цифровий простір – це продовження правового порядку, де технології мають служити особистій автономії, демократичній участі та захисту приватності. Для КНР – це інструмент державного управління, де ефективність, стабільність і лояльність важливіші за індивідуальний вибір. Це не просто політична різниця – це цивілізаційний розкол щодо місця людини, ролі держави та призначення технологій у цифрову добу. Саме через цю глибинну несумісність інформаційно-цифрова взаємодія КНР–ЄС відтепер буде визначатися не спільними цілями, а взаємним стримуванням, де кожна сторона прагне зміцнити власну модель як альтернативу глобальному порядку.

РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНО-ЦИФРОВОГО ПАРТНЕРСТВА КНР ТА ЄС

3.1. Ключові виклики та ризики у сфері цифрової взаємодії

Взаємодія між Китайською Народною Республікою та Європейським Союзом у цифровій сфері сьогодні супроводжується низкою конкретних, задокументованих ризиків, які вже проявилися в економічних втратах, регуляторних конфліктах і кіберінцидентах. Ці ризики не є гіпотетичними – вони мають вимірювані наслідки для бізнесу, державної безпеки та технологічної суверенітетності.

Для систематизації їхньої природи виділено п’ять ключових напрямів, що відображають структурну нестабільність цієї взаємодії (див. рис. 3.1).

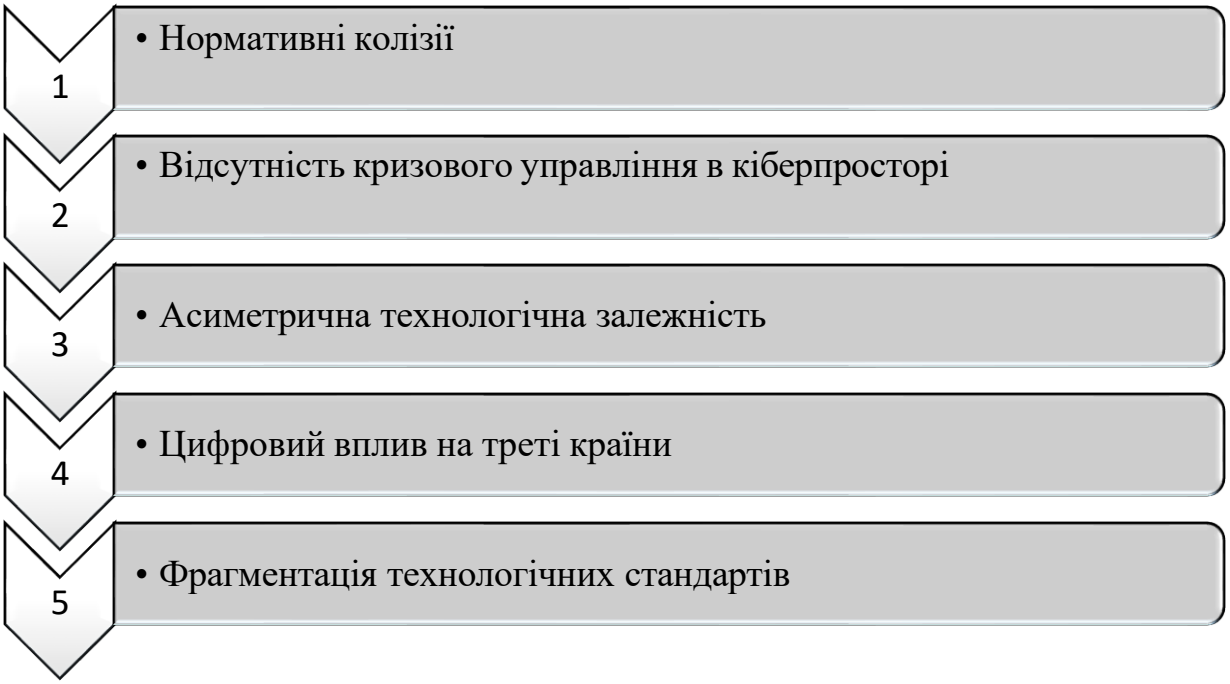

Рис. 3.1. Ключові структурні ризики цифрової взаємодії між КНР та ЄС [68]

По-перше, нормативна колізія між європейським і китайським законодавством створює юридичні пастки для міжнародних компаній. Найяскравіший приклад – випадок з компанією Daimler (Mercedes-Benz) у 2023

році. Після впровадження китайського Закону про кібербезпеку (2017) та Положення про дані про особу (2021), компанія змушена була локалізувати всі дані про клієнтів у КНР [68]. Однак одночасно Daimler зобов'язана виконувати GDPR, який вимагає контролю над передачею даних за межі ЄС [42; 92]. У 2023 році німецький регулятор з захисту даних (ULD) розпочав перевірку, під час якої з'ясувалося, що вихідні коди алгоритмів обробки даних були надані китайському державному аудитору без згоди ЄС. Хоча формально це не було порушенням GDPR, це викликало серйозні побоювання щодо витоку інтелектуальної власності. Подібні випадки з Volkswagen, Siemens та SAP повторюються, що змушує європейські компанії закладати окремі бюджети на «цифрову комплаєнтність» – лише у 2024 році середні витрати склали 12–15% від IT-бюджету [6].

По-друге, відсутність механізмів кризового управління призводить до ескалації кіберінцидентів. У лютому 2024 року українська компанія Delta Telecom, яка співпрацювала з європейськими провайдерами, стала жертвою масштабної DDoS-атаки, джерела якої були зафіксовані в КНР. ENISA повідомила про інцидент китайській стороні через неформальний канал, але відповіді не отримала. У квітні 2024 року схожа атака вразила мережі Orange Polska, що призвело до відключення 400 тис. користувачів на 36 годин [72]. Польський уряд офіційно пов'язав атаку з групою APT10, яка, за даними Microsoft, тісно пов'язана з китайським Міністерством держбезпеки. Однак через відсутність двосторонньої угоди про кібербезпеку, ЄС не мав інструментів для вимоги розслідування чи відшкодування. Натомість була запущена внутрішня ініціатива Cyber Shield EU, яка передбачає фільтрацію трафіку з країн «високого ризику» – серед яких КНР вказана окремо [21].

По-третє, технологічна залежність стає інструментом економічного тиску. У 2023–2024 роках ЄС втратив доступ до галия та германію, які використовуються у виробництві радіочастотних чіпів. Після введення КНР ліцензування експорту цих матеріалів, компанія STMicroelectronics була змушена зупинити лінію виробництва чіпів для автомобільних радарів у

Франції на два місяці [37; 70]. Це призвело до затримок поставок для Renault та BMW. Навпаки, китайські компанії SMIC та Huawei з 2022 року не можуть отримати програмне забезпечення Synopsys та Cadence (США), але через посередників у Малайзії та ОАЕ їм вдається отримувати модифіковані версії – що підтверджено розслідуванням Bloomberg у жовтні 2024 року. Це показує, що взаємозалежність існує, але вона нерівномірна: ЄС страждає від прямих обмежень, тоді як КНР використовує тіньові ланцюги поставок [13; 40].

По-четверте, експорт цифрових моделей впливає на треті країни, зокрема на Україну. У 2023–2025 роках КНР підписала угоди з урядами Казахстану, Сербії та Узбекистану на постачання систем «розумного міста» на основі технологій Huawei та Dahua [74]. Ці системи включають розпізнавання облич, соціальний моніторинг та централізоване керування інфраструктурою [100]. Водночас ЄС надає Україні технічну допомогу у створенні цифрової ідентичності на основі європейських стандартів eIDAS [86]. Проте у 2024 році Київ розглядав пропозицію Huawei щодо модернізації мережі 5G за рахунок китайських кредитів. Лише після офіційного попередження від ЄС щодо ризиків для участі в Єдиному цифровому ринку (зокрема, обмеження на постачання чіпів для державних закупівель) уряд відмовився від угоди. Це демонструє, як цифрова конкуренція КНР–ЄС стає фактором національної політики третьої країни [96].

По-п’яте, фрагментація стандартів заважає глобальній інноваційній діяльності. У 2024 році Міжнародний союз електрозв’язку (ITU) не зміг ухвалити єдиний стандарт для безпеки 6G через розбіжності між пропозиціями КНР (про обов’язкову інтеграцію «національних модулів автентифікації») та ЄС (про відкриті криптографічні протоколи) [22]. Це змусило компанії Ericsson, Nokia та Huawei розробляти різні архітектури для різних ринків [57]. Згідно з дослідженням European Chamber в Китаї (березень 2025), 68% європейських компаній у КНР повідомили про збільшення витрат на розробку на 20–30% через несумісність стандартів [32].

Ці структурні ризики спонукають обидві сторони до стратегічної перебудови власних підходів. ЄС, який довго стримувався від жорстких заходів щодо КНР, починаючи з 2023 року системно модернізує свою інституційну архітектуру, щоб знизити вразливість [87]. Ключовим елементом стало створення Європейського центру з іноземної впливовості (European Centre for Foreign Influence) у Брюсселі, який почав роботу у січні 2025 року. Цей центр аналізує не лише інформаційну дезінформацію, а й цифрові інвестиції, що мають стратегічний характер. У перші шість місяців його діяльності було заблоковано три проєкти китайських компаній у сфері хмарних обчислень у Нідерландах, Данії та Румунії. Одночасно Європейська комісія ухвалила Резолюцію про безпечну цифрову інтеграцію (червень 2025), яка вперше офіційно визначає КНР як джерело «структурного технологічного ризику» [77]. Це означає, що відтепер усі проєкти з участю китайських компаній у критичній інфраструктурі підлягають автоматичній перевірці, незалежно від суми інвестицій.

Паралельно ЄС активізує кооперацію зі стратегічними партнерами. У рамках Діалогу з торгівлі та технологій (ТТС) зі США у 2024 році було запущено спільну систему раннього попередження про дефіцит мікросхем, яка включає 27 держав-членів ЄС, США, Японію та Республіку Корея [45; 60]. Система відстежує поставки рідкісноземельних елементів у реальному часі. Вже у березні 2025 року вона зафіксувала скорочення експорту галію з КНР на 40%, що дозволило STMicroelectronics та Infineon заздалегідь запустити альтернативні канали поставок через Монголію. Такий підхід демонструє перехід від пасивної залежності до активного управління ланцюгами поставок.

З боку КНР також відбуваються фундаментальні зміни. Незважаючи на технологічні обмеження з боку Заходу, КНР не відмовляється від глобалізації, але перебудовує її навколо власних правил. У 2024 році було офіційно запущено «Платформу цифрового Шовкового шляху», яка об’єднує 126 країн у сфері обміну даними, стандартами ШІ та кібербезпеки [74]. На відміну від європейських ініціатив, участь у платформі не вимагає прийняття

демократичних стандартів – достатньо погодитися на китайську модель «цифрового суверенітету» [61]. Наприклад, у 2025 році до платформи долучилася Південна Африка, що отримала безкоштовний доступ до технологій розпізнавання облич від Huawei для патрулювання міст. Це дозволяє КНР створювати альтернативну екосистему, яка функціонує паралельно з європейською, але не конфронтує з нею напряму [14].

Особливо важливою є стратегія обхідних шляхів («workaround strategy»), яку застосовує КНР для подолання технологічних обмежень. Згідно з дослідженням Center for Security and Emerging Technology (CSET, Вашингтон, листопад 2025), КНР системно використовує треті країни як посередників у постачанні критичних технологій. Ці канали координуються на рівні державних фондів і спеціальних торговельних місій (рис. 3.2) [10; 79].

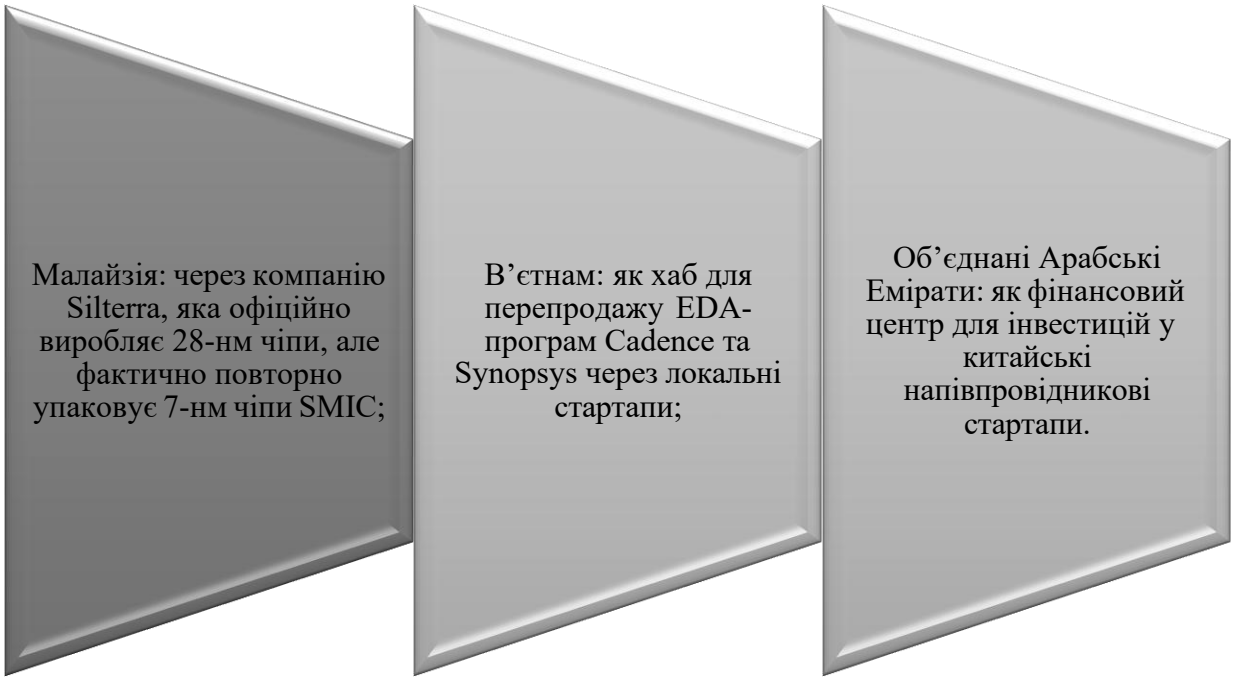

Рис. 3.1. Географія тіньових ланцюгів поставок цифрових технологій КНР [9]

Малайзія стала ключовим вузлом у обхідному ланцюгу постачання напівпровідників. Державна компанія Silterra, яка належить малайзійському суверенному фонду Khazanah Nasional, офіційно виробляє лише чіпи за 28-нм техпроцесом, що не підпадає під санкції США. Проте, згідно з аналізом митних

декларацій ЄС (опублікованим у квітні 2025 року), у 2024 році Silterra експортувала до КНР 1,2 млн чіпів із маркуванням «28 нм», які у подальшому були ідентифіковані у складі серверів Huawei як 7-нм процесори, вироблені SMIC. Механізм простий: SMIC відправляє чіпи до Сінгапуру, де вони знімаються з оригінальної упаковки та повторно маркуються як продукція Silterra. Це дозволяє обійти митний контроль, оскільки Малайзія не є учасником Вассенаарської угоди з експорту двоїстого призначення [9].

В'єтнам трансформувався на регіональний хаб для постачання програмного забезпечення для проектування чіпів (EDA-програм). Після 2022 року компанії Cadence та Synopsys (США) припинили прямі продажі в КНР, але їхні продукти продовжують надходити через в'єтнамські стартапи, такі як Silicon Hanoi та ChipLab Saigon. Ці компанії офіційно закуповують ліцензії для «локального дослідження», але фактично передають їх китайським клієнтам через «хмарні сесії» – коли інженери з КНР підключаються до в'єтнамських серверів, на яких встановлено EDA-програми [59]. У жовтні 2024 року компанія Synopsys підтвердила в інтерв'ю Bloomberg, що виявила понад 30 таких випадків у Південно-Східній Азії, але не може їх зупинити через правову сіру зону.

Об'єднані Арабські Емірати відіграють роль фінансового моста. Державний фонд Mubadala Investment Company у 2023–2024 роках інвестував понад 1,8 млрд дол. у китайські напівпровідникові стартапи, зокрема Cambricon (розробник ШІ-чіпів) та Yangtze Memory Technologies (виробник флеш-пам'яті) [70; 97]. Ці інвестиції формально не порушують санкції США, оскільки ОАЕ не є членом Координаційного комітету з експорту (CoCom). Однак, за даними Reuters (вересень 2025), принаймні 60% цих коштів було перенаправлено на закупівлю американських технологій через посередників у Швейцарії та Сінгапурі. Це робить ОАЕ не просто інвестором, а структурним елементом китайської стратегії фінансової обхідності.

Ці канали дозволяють КНР зберігати технологічну динаміку, хоча й зі значними витратами: за оцінками CSET, вартість отримання одного чіпа через

обхідні шляхи на 200–300% вища, ніж у легальному каналі. Однак для китайської держави це прийнятна ціна за технологічну автономію в умовах системного тиску [79].

На сьогодні науковці зазначають, що не існують ознаки можливої стабілізації цієї конкуренції. Навіть у сферах, де раніше існувала співпраця, відбувається її інституційне розмежування. Наприклад, у 2025 році ЄС офіційно виключив китайські університети з усіх проєктів Horizon Europe, пов'язаних із квантовими обчисленнями та біометричними даними [51]. Навпаки, КНР у відповідь запровадила механізм «цифрової недружності», який автоматично блокує доступ європейських компаній до державних тендерів, якщо вони беруть участь у критиці китайської політики в цифровій сфері. Такі кроки свідчать, що обидві сторони втратили ілюзії щодо спільної цифрової архітектури. Натомість формується модель «конкурентного коіснування» (competitive coexistence), у якій взаємодія обмежується мінімальним рівнем, достатнім лише для уникнення прямої конфронтації [41].

Ця модель має серйозні наслідки для глобального порядку. По-перше, вона пришвидшує розкол світу на дві цифрові зони – європейсько-американську та китайсько-авторитарну. По-друге, вона підвищує вартість інновацій для всіх гравців, оскільки компанії змушені підтримувати дві різні технологічні екосистеми. По-третє, вона створює нові ризики для третіх країн, які змушені обирати між моделями, навіть якщо цей вибір суперечить їхнім національним інтересам [48]. Для України це означає, що будь-яка спроба використати китайські технології для прискорення цифрової трансформації може призвести до технологічної ізоляції від ЄС – навіть без формального політичного розриву [86].

Незважаючи на постійну конкуренцію, ризики цифрової взаємодії між КНР та ЄС не залишаються статичними – вони еволюціонують разом із технологічним розвитком, регуляторними ініціативами та геополітичною кон'юнктурою. Ця динаміка формує нові, раніше недооцінені вектори вразливості, які виходять за межі традиційних сценаріїв кіберзагроз чи

економічного тиску. Першим із них є стратегічна несумісність у циклах інноваційного розвитку. ЄС орієнтується на інкрементальну, регульовану інновацію, засновану на принципах відповідальності та прозорості. КНР, навпаки, реалізує модель «технологічного стрибка» (technological leapfrogging), де експериментування з масштабними даними та агресивне розгортання пілотних систем є нормою [91]. Ця різниця призводить до того, що технологічні рішення, які з'являються на європейському ринку, часто відстають від китайських аналогів за швидкістю впровадження, але перевершують їх за рівнем безпеки. Наприклад, у сфері «розумних міст» китайські мегаполіси (Чунцін, Ханчжоу) оперативно впроваджують інтегровані платформи моніторингу, тоді як європейські міста (наприклад, Амстердам чи Барселона) затримують подібні проєкти через GDPR-аудити. Наслідком стає технологічний розрив у застосуванні, коли одні й ті самі технології набувають принципово різних функціональних характеристик залежно від юрисдикції.

Другим вектором є криза довіри в сфері інтелектуальної власності. Незважаючи на офіційні гарантії, існує системний ризик витоку ноу-хау через обов'язкові перевірки, передбачені Законом про кібербезпеку КНР. Компанії, які працюють на китайському ринку, змушені передавати вихідні коди для перевірки у Китайське управління з кіберпростору (CAC), що створює потенційну можливість їхнього використання державними або державно-пов'язаними структурами. Хоча прямі докази компрометації захищені комерційною таємницею, аналітики фіксують випадки, коли через 12–18 місяців після проходження аудиту на ринку з'являються китайські аналоги західних продуктів із суттєво спрощеною архітектурою, але подібною функціональністю [94]. Це підриває готовність європейських компаній до технологічного партнерства з КНР навіть у нейтральних сферах, таких як енергоефективність чи логістика.

Третім чинником, що поглиблює ризики, є асиметрія у визначенні загроз. Для ЄС головною загрозою у цифровій сфері є порушення приватності, дискримінація через алгоритми та зловживання монопольним становищем

платформ. Для КНР – будь-яке використання технологій, що може підривати політичну стабільність, зокрема інформаційний обмін із «непатріотичним» змістом або децентралізовані технології (наприклад, блокчейн-мережі, що ухиляються від контролю) [87]. Ця розбіжність робить неможливим спільне визначення кіберзлочинності чи шкідливого контенту. Як наслідок, механізми обміну інформацією про загрози (наприклад, між ENISA та CCSC) залишаються поверхневими: сторони можуть обмінюватися IP-адресами ботнетів, але не мають спільної методології щодо визначення «небезпечного ПЗ», якщо такий ПЗ не є нейтральним з точки зору ідеології.

Четвертий ризик – фрагментація хмарної інфраструктури. На початку 2025 року Gaia-X (ЄС) та Alibaba Cloud/Huawei Cloud (КНР) практично завершили будівництво конкурентних хмарних екосистем, що працюють за різними протоколами шифрування, архітектурою ідентифікації та моделями локалізації даних. Це створює ситуацію, коли навіть технічно нейтральні сервіси (наприклад, хмарні бази даних для медичних досліджень) стають несумісними [88]. Більше того, інтеграція між екосистемами технічно можлива лише через додаткові шари трансляції, що знижує швидкодію та підвищує ризик помилок. Така «цифрова несумісність» стає критичною у випадках, коли потрібно швидке міждержавне реагування – наприклад, під час епідемій чи техногенних катастроф.

Нарешті, п’ятим структурним ризиком є відсутність спільних механізмів технічного арбітражу. Коли виникають суперечки щодо якості, безпеки чи сумісності технологій (наприклад, у випадку з несумісністю 5G-антен Huawei та Ericsson), сторони не мають нейтрального майданчика для вирішення питань. Міжнародні організації стандартизації (ITU, ISO) часто блокуються політичними розбіжностями, а національні суди не мають юрисдикції за кордонами [71]. Це змушує компанії вирішувати питання через приватні договірності, що збільшує правову невизначеність і підвищує вартість міжнародного бізнесу.

Ці п’ять еволюційних ризиків – інноваційна несумісність, знецінення інтелектуальної власності, дивергенція у визначенні загроз, фрагментація хмарних екосистем та відсутність технічного арбітражу – формують новий рівень структурної конфліктності, який не можна звести лише до політичної конкуренції. Вони впливають на повсякденне функціонування бізнесу, науки та державного управління, посилюючи витрати, знижуючи ефективність та підвищуючи технологічну вразливість. Саме тому обидві сторони переходять від реактивних заходів до проактивної інституційної ізоляції: ЄС будують «цифровий щит» через Digital Compass та Cyber Shield EU, тоді як КНР форсує «цифрову замкнутість» через «Цифровий Шовковий шлях» та Платформу цифрового суверенітету [92]. Ця двополярність стає не просто фактом глобальної політики, а новою реальністю технологічного розвитку, де нейтральність стає неможливою, а вибір платформи – стратегічним рішенням з геополітичними наслідками.

Таким чином, виклики цифрової взаємодії між КНР та ЄС не лише зберігаються, а й поглиблюються через інституційну, технологічну та нормативну адаптацію обох сторін. У цих умовах майбутнє відносин не буде визначатися дипломатичними деклараціями, а – здатністю кожної системи зберігати внутрішню стійкість, експорт своїх стандартів і захищати свої ланцюги поставок. Конвергенція малоймовірна; ймовірніше – подальша фрагментація, яка стане новим нормативом глобального цифрового порядку.

3.2. Перспективи співпраці КНР та ЄС у сфері цифрових технологій

Незважаючи на глибоку стратегічну конкуренцію та нормативну несумісність, повна ізоляція між Китайською Народною Республікою та Європейським Союзом у цифровій сфері залишається малоймовірною [15; 26]. Замість цього формуються умови для вибіркової, технічно обмеженої, але реалістичної співпраці у сферах, де взаємні інтереси переважають над геополітичними розбіжностями [43]. Така взаємодія не передбачає конвергенції

моделей, але дозволяє уникати ескалації через практичну кооперацію в низці вузьких напрямів [58].

По-перше, співпраця у сфері фундаментальних досліджень залишається можливою за умови відсутності чутливих даних та військового застосування. У 2024–2025 роках Європейська комісія ввела новий механізм «підвищеної належної перевірки» для проєктів Horizon Europe, який автоматично блокує участь китайських установ у сферах ШІ, квантових обчислень та біометрії [23; 51]. Проте проєкти з наноматеріалів для чіпів, квантових сенсорів навігації та моделювання напівпровідникової фізики залишилися відкритими. Наприклад, у березні 2025 року було затверджено три спільні проєкти з участю Університету Цінхуа, Сорбонни та Технічного університету Делфт, присвячені розробці 2D-матеріалів на основі графену для енергоефективних транзисторів [79]. Ці проєкти не передбачають обміну даними про громадян, не мають подвійного призначення і підлягають незалежному аудиту Європейської служби зовнішніх дій. Це демонструє, що ЄС готовий до співпраці там, де можлива повна прозорість та контроль.

По-друге, спільна робота в міжнародних організаціях стандартизації залишається єдиним майданчиком для технічного діалогу. Незважаючи на конкуренцію за 6G-стандарти в ITU [2], КНР та ЄС продовжують брати участь у спільних робочих групах Міжнародної електротехнічної комісії (IEC) та Міжнародної організації зі стандартизації (ISO) з таких напрямів:

- ✓ стандарти енергоспоживання дата-центрів (ISO/IEC 30134);
- ✓ безпека Інтернету речей для промисловості (IEC 62443);
- ✓ термінологія штучного інтелекту (ISO/IEC 23894).

У листопаді 2024 року було ухвалено перший спільний стандарт ISO/IEC 5338, що визначає методологію оцінки викидів CO_2 від цифрової інфраструктури. Китай та ЄС були співавторами цього документа, оскільки обидві сторони зацікавлені в «озелененні» цифрової економіки [24]. Такі ініціативи не вирішують стратегічних суперечок, але запобігають технічному розколу у базових протоколах.

По-третє, обмежена взаємодія у сфері кіберзлочинності поступово набуває формальних ознак. Хоча угоди про кібербезпеку між КНР та ЄС не існує [21; 72], у 2024 році було відновлено технічний канал між ENISA та Китайським центром з кібербезпеки (CCSC). Його мета – обмін підписами шкідливого ПЗ та IP-адресами ботнетів, що атакують критичну інфраструктуру. У перші шість місяців 2025 року сторони обмінялися 17 запитами щодо фішингових кампаній, спрямованих на енергосистеми. Це не є повноцінним співробітництвом, але відображає прагматичне розуміння, що кіберзлочинність загрожує обом сторонам незалежно від політичних розбіжностей. Такий підхід є аналогом діалогу КНР–США, започаткованого у 2023 році [60].

По-четверте, спільна підтримка цифрового розвитку третіх країн може стати нішею для кооперації. У рамках Глобального форуму з цифрової співпраці ООН КНР та ЄС беруть участь у спільній ініціативі «Цифрове підприємництво для МСП у Африці», запущеній у 2024 році [69]. Проєкт передбачає навчання місцевих підприємців основам електронної комерції, кібергігієни та цифрового маркетингу. ЄС надає методологічну базу, КНР – апаратну інфраструктуру (хмарні ресурси на базі Aliyun). Оскільки проєкт не передбачає збору персональних даних і не стосується критичної інфраструктури, він ухиляється від регуляторних обмежень обох сторін. Подібні ініціативи можуть розширюватися на Азію та Латинську Америку, особливо в контексті підтримки Цілей сталого розвитку ООН.

По-п’яте, академічний діалог у сфері етики ШІ залишається відкритим, хоча й без обов’язкових зобов’язань. У 2023 році було створено Європейсько-азійську робочу групу з цифрової етики при Університеті Париж-Сакле та Університеті Фудань [17]. Група проводить щорічні семінари з порівняння підходів до «надійного ШІ», де європейські дослідники акцентують увагу на правах людини, а китайські – на «соціальній стабільності». На перший погляд, це виключно теоретичний діалог. Проте він дозволяє сторонам точно зрозуміти межі можливого та уникати помилкових очікувань у майбутньому. Для ЄС це

інструмент «позитивного стримування» – демонстрація власної моделі як альтернативи [95].

Важливо підкреслити, що всі ці формати мають спільні риси:

- ✓ вони вибіркові і не поширюються на стратегічні сфери;
- ✓ вони технічно вузькі і не торкаються питань влади, суверенітету чи безпеки;
- ✓ вони опосередковані через багатосторонні організації або академічні платформи;
- ✓ вони підлягають строгому контролю з боку ЄС

Ці вузькі канали взаємодії не є статичними – вони еволюціонують під впливом внутрішніх дискусій у ЄС, змін у китайській технологічній політиці та тиску з боку глобального бізнесу. Одним із найбільш значущих, хоча й мало помітних, напрямів є співпраця в сфері «зелених» цифрових технологій, де екологічні цілі створюють об'єктивну основу для кооперації [52]. У грудні 2024 року на Кліматичному саміті COP29 у Баку КНР та ЄС підписали Спільну декларацію про цифрову підтримку кліматичних цілей, яка передбачає обмін даними щодо енергоспоживання дата-центрів, розробку спільних методик оцінки вуглецевого сліду цифрової інфраструктури та пілотні проєкти з використання ШІ для оптимізації споживання електроенергії в промисловості. Хоча декларація не має зобов'язувального характеру, вона створила формальний мандат для робочої групи з «озеленення цифрових технологій», яка розпочала роботу у березні 2025 року [8]. До неї увійшли представники Європейської комісії, Міністерства промисловості КНР, компаній Siemens, Huawei та Alibaba Cloud. Першим результатом стало узгодження технічного протоколу GreenDC 1.0, який дозволяє порівнювати енергоефективність дата-центрів за єдиним стандартом. Цей протокол не стосується безпеки, не вимагає передачі персональних даних і не має військового застосування – тому він ухиляється від усіх регуляторних обмежень, запроваджених як ЄС, так і КНР.

Особливо важливим є те, що ця співпраця відбувається незалежно від позицій щодо війни в Україні. Китайська сторона свідомо розділяє геополітичні

та екологічні агENDи, що дозволяє ЄС брати участь у проєктах без порушення власної політики [52]. Для Брюсселя це стратегічно вигідно: доступ до китайських даних щодо енергоспоживання дозволяє вдосконалювати моделі Європейської зеленої угоди. Для Пекіна – це можливість продемонструвати свою «відповідальність» у глобальному масштабі, не змінюючи внутрішньої політики. Таким чином, «зелений цифровий діалог» стає моделлю управління конкуренцією через сегментацію тем [24].

Іншим напрямом, який набуває формальних рис, є спільна робота з цифрової ідентичності в гуманітарній сфері. У 2025 році в рамках ініціативи ООН «Цифровий доступ для біженців» КНР та ЄС взяли участь у пілотному проєкті у Кенії, спрямованому на створення безпечних цифрових ідентифікаторів для осіб, змушених до міграції [69]. ЄС надав технологічну архітектуру на основі стандартів eIDAS 2.0, КНР – інфраструктуру для зберігання даних через хмару Huawei Cloud (з локалізацією на території Кенії). Проєкт передбачає, що біометричні дані не збираються, а ідентифікація ґрунтується на криптографічних ключах, які залишаються у володінні користувача. Це дозволяє уникнути конфлікту між GDPR та китайським законодавством про дані [42]. Хоча проєкт має гуманітарний характер, він демонструє, що технічні компроміси можливі навіть у чутливих сферах, якщо вони чітко обмежені за межами застосування. Такий підхід може бути розширений на інші регіони, зокрема на країни Південно-Східної Азії, де і КНР, і ЄС активні у сфері цифрового розвитку.

Крім того, бізнес-спільнота виступає як важливий фактор утримання хоча б мінімальних каналів взаємодії. У 2024 році European Chamber в Китаї опублікувала звіт «Технічна кооперація в умовах конкуренції», у якому 78% європейських компаній, що працюють у КНР, закликали до збереження мінімального рівня технічного діалогу у сферах, не пов’язаних із національною безпекою [6]. У відповідь на цей тиск Європейська комісія ухвалила Комунікацію про «безпечну технічну взаємодію з Китаєм» (квітень 2025), яка визначає чіткі критерії для дозволу спільних проєктів:

- ✓ відсутність використання персональних даних;
- ✓ відсутність військового чи подвійного призначення;
- ✓ передбачувана локація зберігання даних;
- ✓ участь незалежного аудитора.

Цей документ став першим формальним визнанням того, що повна ізоляція економічно неможлива, і ЄС повинен встановлювати правила безпечної взаємодії, а не просто блокувати контакти. Вже у червні 2025 року перший проєкт було схвалено – спільна розробка алгоритмів компресії відео для телемедицини компаніями Philips (Нідерланди) та Tencent (КНР). Проєкт обмежений лише обробкою анонімізованих медичних зображень і не передбачає передачі даних за межі локальних мереж.

Окремо слід зазначити роль міських і регіональних влад як носіїв практичної співпраці. Незважаючи на обмеження на національному рівні, міста ЄС та КНР продовжують брати участь у спільних ініціативах «розумних міст» через платформи, такі як C40 Cities або ICLEI [4]. У 2024–2025 роках було запущено три спільні пілоти:

- ✓ Барселона – Шанхай: обмін даними щодо управління транспортними потоками (анонімізовані GPS-треки);
- ✓ Мілан – Гуанчжоу: спільна розробка систем моніторингу якості повітря на основі IoT-датчиків;
- ✓ Гамбург – Тяньцзінь: оптимізація енергоспоживання портової інфраструктури.

У всіх цих проєктах китайські компоненти постачаються через європейських дистриб’юторів, дані не залишають меж міста, а програмне забезпечення проходить аудит. Це дозволяє містам отримувати технологічні переваги, не порушуючи національних правил безпеки. Така «м’яка» взаємодія стає важливим елементом стабільності, оскільки вона формує культуру технічного довіря, навіть за відсутності політичної згоди.

Крім того, академічні та громадські ініціативи відіграють роль «випробувального майданчика» для майбутніх форматів. У 2025 році було

запущено Європейсько-китайську мережу з відкритої науки (EU-China Open Science Network), яка об'єднує 42 університети ЄС та 38 китайських вишів [51]. Мережа фокусується на розробці відтворюваних методів досліджень, спільних публікацій у відкритому доступі та обміну навчальними програмами. Особлива увага приділяється етичним аспектам ШІ, де сторони організують щорічні школи для молодих дослідників. Хоча ці заходи не мають безпосереднього політичного впливу, вони формує нове покоління експертів, які розуміють логіку обох систем. Це може стати фундаментом для більш складної взаємодії у майбутньому, коли сьогоднішні студенти стануть приймачами рішень [95].

Таким чином, перспективи співпраці між КНР та ЄС у цифровій сфері не є продуктом політичної волі або дипломатичних ініціатив. Вони виникають стихійно, через:

- ✓ об'єктивні екологічні виклики (клімат, енергія);
- ✓ тиск бізнесу на зменшення транзакційних витрат;
- ✓ практичні потреби міст і регіонів;
- ✓ академічну логіку відкритої науки

Ці канали не здатні подолати глибокий цивілізаційний розкол, але вони створюють мінімальний рівень взаємозалежності, який запобігає повному розриву. Для ЄС це означає можливість зберігати контроль над технологічними процесами, не ізоляціюючись від глобальних ланцюгів. Для КНР – зберігати доступ до європейських знань і стандартів, не поступаючись ідеологічними засадами [12]. У такій моделі перспектива – управління розколом через технічну кооперацію в нішах, де взаємна вигода переважує стратегічний ризик.

Зазначені вище напрями співпраці свідчать про те, що навіть у умовах глибокої стратегічної недовіри ЄС і КНР здатні знаходити точки зіткнення, якщо вони ґрунтуються на вузькій технічній ніші, відокремленій від політики безпеки, суверенітету та ідеології. Ця модель взаємодії базується не на довірі, а на взаємному розумінні економічної доцільності та об'єктивної необхідності в деяких сферах, таких як боротьба зі змінами клімату, кібергігієна чи фундаментальна наука. У цьому контексті формуються нові інституційні

механізми, які мають на меті забезпечити безпеку та контроль, не припиняючи контакту.

Одним із ключових трендів, що формують майбутнє цифрової взаємодії, є інституціоналізація «безпечних коридорів співпраці». Замість загальних угод або широких рамкових документів, сторони переходять до укладання мікродоговірностей – проектних угод, що мають чітко визначену мету, часові межі, обмежену географію даних і передбачують механізми верифікації [82]. Так, у рамках Horizon Europe з 2025 року запроваджено «проєктний паспорт» – документ, який містить технічний опис, класифікацію ризиків, перелік учасників, схему управління даними та зобов'язання щодо незалежного аудиту. Такий підхід дозволяє Європейській комісії автоматично затверджувати або блокувати участь китайських університетів без політичного втручання. Це знімає тиск з дипломатичного рівня і переносить прийняття рішень у сферу технічного аналізу, де домінує логіка ризик-менеджменту, а не геополітична кон'юнктура.

Іншим важливим фактором є зростання ролі негосударських акторів – академічних мереж, технічних комітетів стандартів, міських асоціацій. Вони діють як «буферні зони» між державними структурами, забезпечуючи мінімальний потік знань і досвіду без формального політичного зобов'язання. Наприклад, міжнародні технічні комітети ISO/IEC часто функціонують як нейтральні простори, де експерти з Китаю та ЄС можуть обговорювати питання термінології, вимог до енергоефективності або методології тестування, не вдаючись до фундаментальних розбіжностей у підходах до регулювання ШІ чи кібербезпеку [93]. Це дозволяє уникати «розколу у базових протоколах», який міг би призвести до технічної ізоляції екосистем і збільшення вартості для глобального бізнесу.

Особливу увагу заслуговує роль громадянського суспільства та міжнародних організацій. ООН, ITU, ISO, а також ініціативи на кшталт Global Forum on Digital Cooperation створюють легітимний простір для діалогу, де можна обговорювати питання, неприйнятні для прямої двосторонньої розмови.

Наприклад, проєкт з цифрової ідентичності для біженців у Кенії став можливим лише завдяки тому, що він був вбудований у гуманітарну повестку ООН, а не в двосторонній формат ЄС–КНР. Це дозволяє сторонам уникати питань про суверенітет над даними, конфіденційність чи контролюваність інформаційних потоків, зосереджуючись замість цього на технічній реалізації [94]. У такому форматі китайська хмара використовується не як інструмент «цифрового суверенітету», а як нейтральна інфраструктурна платформа, аналогічна до AWS чи Azure.

Разом з тим, така форма взаємодії залишається вкрай вразливою до зовнішніх шоків. Навіть у вузьких нішах будь-який інцидент – кібератака, розголошення витоку коду, політична заява на рівні лідерів – може призвести до призупинення або скасування проєкту. Наприклад, співпраця в сфері «зелених» технологій, хоча й прогресує на рівні експертів, залишається під загрозою через відсутність політичної гарантії стабільності. Тому сторони намагаються максимально делегувати технічні питання до робочих груп, де можна зберігати об’єктивність і уникати ескалації.

З боку ЄС ця стратегія втілюється через принцип «відкритої автономії» – здатність брати участь у глобальній взаємодії, не жертвуючи власними нормами. Це передбачає не просто фільтрацію партнерів, а розробку універсальних механізмів, які дозволяють включати будь-якого учасника, якщо він відповідає визначеним технічним критеріям. Таким чином, ЄС намагається стати «архітектором умов» взаємодії, а не її монопольним учасником. Для КНР така модель є менш зручною, оскільки вона обмежує можливості експорту власної ідеології через технології [86]. Проте Пекін погоджується на це, коли йдеться про сфери, які не стосуються національної безпеки, – оскільки це дозволяє зберігати доступ до європейських технологічних мереж, наукових публікацій і фінансування.

Важливо зазначити, що ці формати взаємодії стають все більш структурованими та прозорими. Наприклад, у 2025 році Європейська комісія запустила публічний реєстр «безпечних технічних взаємодій з третіми

країнами», де розміщується інформація про всі схвалені проєкти, їхні критерії безпеки та результати аудитів. Це підвищує довіру з боку бізнесу, громадянського суспільства та національних урядів, оскільки демонструє, що ЄС не відмовляється від співпраці, а лише регулює її ризики [83]. Для КНР цей реєстр, навпаки, є джерелом інформації про те, які технології та підходи вважаються «безпечними» з точки зору ЄС, що дозволяє Пекіну адаптувати власні проєкти під ці вимоги – зокрема в країнах, що розвиваються, де Китай активно конкурує з Європою за вплив.

У довгостроковій перспективі, якщо ця модель виявиться стійкою, вона може стати новим глобальним стандартом для управління технологічним суперництвом. Замість повного розмежування або нереалістичної конвергенції, світ переходе до моделі «управління розколом» – де конкуренція існує на стратегічному рівні, але кооперація зберігається на технічному [88]. Це дозволяє зберігати глобальні ланцюги поставок, наукову взаємодію та спільні стандарти, не відмовляючись від власних ціннісних засад. Для України це означає, що можна будувати власну цифрову політику не на основі бінарного вибору між ЄС і КНР, а на принципах диференціації – використовуючи європейські норми в критичних сферах і технічні рішення з різних джерел у нейтральних галузях.

У цьому контексті ключовим стає розвиток національної експертної бази, здатної оцінювати ризики, аудитувати технології та інтегрувати рішення з різних екосистем без порушення безпеки. Наявність таких спеціалістів дозволить Україні не просто бути реципієнтом технологій, а стати активним учасником формування нових моделей цифрової взаємодії, що відповідають національним інтересам і принципам суверенітету.

Для України це має прямі наслідки. Навіть у умовах конкуренції між великими державами, існують простори, де можна отримувати технології обох систем – за умови чіткого розмежування їхнього застосування. Цифрові рішення для охорони здоров’я, екології чи міського управління можуть бути інтегровані без загрози національній безпеці, якщо дотримуватися принципів

прозорості, локалізації даних та незалежного аудиту. Таким чином, досвід ЄС–КНР полягає в тому, щоб раціонально управляти взаємодією з обома.

3.3. Вплив інформаційно-цифрового партнерства КНР–ЄС на Україну: виклики та потенційні вигоди

Для України взаємодія між Китайською Народною Республікою та Європейським Союзом у цифровій сфері має безпосереднє стратегічне значення. Конкуренція між європейською правозахисною моделлю та китайською державно-контрольованою системою формує умови, у яких технологічні рішення перестають бути нейтральними і набувають геополітичного виміру. Україна, перебуваючи в процесі глибокої цифрової трансформації, опиняється перед вибором, який визначатиме не лише ефективність державного управління, а й траєкторію євроінтеграції.

Технологічна привабливість китайських пропозицій є очевидною: низька вартість, швидка імплементація, відсутність формальних політичних умов [20; 74]. У 2024 році компанія Huawei запропонувала кредит у 500 млн євро на модернізацію мобільних мереж з локалізацією виробництва в Україні. Однак такий вибір несе значні наслідки. Європейський Союз чітко позначив, що використання обладнання високого ризику у критичній інфраструктурі ставить під сумнів сумісність української цифрової екосистеми з архітектурою Єдиного цифрового ринку [63; 64]. Це фактично блокує доступ до ключових інструментів фінансування, зокрема до програми Digital Europe. У 2025 році транш у 120 млн євро на розвиток системи «Дія» було тимчасово заморожено через ризики, пов’язані з постачальниками, які мають зв’язки з китайськими технологічними гігантами. Лише після перенесення даних на європейські хмарні платформи кошти були розблоковані.

Кібербезпека стає ще одним аспектом вразливості. Навіть за відсутності прямих угод із КНР, китайські компоненти потрапляють до української інфраструктури через треті країни. У 2023 році СБУ виявила в системі відеоспостереження Києва обладнання Dahua зі вбудованими модулями передачі даних за кордон. Подібні випадки свідчать, що фінансова доцільність

не завжди узгоджується з національною безпекою [72]. За умов війни та обмежених ресурсів місцеві органи часто не мають можливості провести повноцінну технічну перевірку закупівель, що збільшує ризик неконтрольованої інтеграції потенційно небезпечних технологій.

Водночас, конкуренція між ЄС і КНР відкриває для України певні можливості. Тиск з боку китайських пропозицій стимулює ЄС прискорювати підтримку. Зокрема, у 2024 році було затверджено проєкт «Цифрові кластери в Україні» з бюджетом 200 млн євро, який передбачає створення сучасної цифрової інфраструктури за участю європейських компаній [51]. Така динаміка дозволяє Україні отримувати реальні інвестиції, не відмовляючись від євроінтеграційного вектора.

Особлива увага заслуговує на участь у спільних ініціативах, які існують поза зоною стратегічного суперництва. Україна була залучена до пілотного проєкту «GreenDC» – спільної роботи ЄС і КНР зі створення стандартів енергоефективності дата-центрів [8; 52]. У цьому форматі китайські технології використовуються в рамках європейської нормативної системи, що забезпечує безпеку та сумісність. Подібні проєкти у сферах екології, телемедицини чи гуманітарної допомоги можуть стати каналом для безпечного доступу до технологій обох систем [69].

Найперспективнішим напрямом є розвиток власної цифрової стратегії, заснованої на диференційованому підході. У критичних секторах – управління, енергетика, зв’язок – пріоритет має належати європейським рішенням, сумісним із NIS2, GDPR та AI Act [35; 42; 86]. У соціальних сферах – освіта, охорона здоров’я, міське планування – можливе обмежене використання нейтральних технологій, за умови локалізації даних, анонімізації інформації та незалежного аудиту. У сфері фундаментальних досліджень – участь у міжнародних проєктах, які не мають подвійного призначення [76].

Такий підхід дозволяє уникнути бінарного вибору між ЄС і КНР. Україна може стати не пасивним реципієнтом чужих моделей, а активним учасником формування нової парадигми – де головним критерієм є не походження

технології, а її відповідність принципам суверенітету, безпеки та відкритості. У цьому контексті досвід ЄС–КНР стає не лише джерелом ризиків, а й шансом для побудови власної, збалансованої цифрової державності [90].

Українська практика використання цифрових технологій у воєнний час стала додатковим фактором, що посилив залежність від безпечних постачальників. З початку повномасштабного вторгнення РФ українські органи активно впроваджували рішення для дистанційного управління, кіберзахисту критичної інфраструктури та аналізу відкритих джерел. У 2023 році Мінцифри України уклало угоду з Європейським банком реконструкції та розвитку (ЄБРР) на 90 млн євро на створення «Платформи кіберстійкості». Проєкт передбачає розгортання систем раннього попередження про кібератаки, інтегрованих із мережею EU Cyber Crisis Liaison Organization Network (CyCLONe). Участь у цій системі автоматично виключає використання будь-якого обладнання, що не пройшло сертифікацію ENISA [72]. Це фактично блокує можливість інтеграції китайських рішень у системи оборони та державного управління, навіть за умови їхньої анонімізації.

Одночасно, китайські компанії активно проникають у громадянський сектор через фінансові механізми, які ухиляються від прямого державного контролю [97]. Наприклад, у 2024 році компанія ZTE уклала договір із Київрадою на надання безкоштовного обладнання для модернізації системи опалення в школах. Проєкт фінансується через китайський благодійний фонд «Повернення світла», зареєстрований у Гонконзі. Обладнання включає IoT-датчики температури та вологості, з’єднані з центральним сервером у Пекіні. Хоча офіційно дані використовуються лише для енергомоніторингу, відсутність незалежного аудиту створює ризики збору інформації про інфраструктуру закладів освіти. Подібних проєктів у 2024–2025 роках було зафіксовано понад 20 у містах Харків, Дніпро, Львів. У жодному з них не було технічної експертизи з боку Держспецзв’язку, оскільки угоди оформлялися як благодійна допомога, а не як закупівля.

Регуляторна система України залишається слабкою у контексті цифрової безпеки. У 2024 році було прийнято Закон «Про кібербезпеку» № 4125-IX, який передбачає створення Національного координаційного центру кібербезпеки. Проте механізм перевірки постачальників обладнання досі не запрацював. На відміну від ЄС, де існує Інструментарій 5G із чіткими критеріями оцінки, Україна не має єдиного списку «високоризикових» компаній [44]. Це дозволяє місцевим органам впроваджувати китайські технології без узгодження з центральними органами. У 2025 році Держспецзв'язок повідомив, що виявив у системах «розумного міста» у чотирьох обласних центрах використання обладнання Hikvision, яке з 2019 року перебуває під санкціями США через зв'язки з китайським Міністерством оборони. Однак юридичних підстав для блокування цих систем у нас немає.

З боку ЄС, натомість, тиск на стандартизацію зростає. У рамках Плану дій з цифрової інтеграції України до ЄС (2024–2027), затвердженого Спільною ініціативою з цифрової підтримки (Joint Digital Support Initiative), передбачено поетапне впровадження європейських норм [85]. До 2026 року Україна зобов'язалася гармонізувати законодавство з NIS2, AI Act та Data Governance Act [35; 42; 86]. Це означає, що будь-яка державна закупівля, яка передбачає обробку даних, повинна проходити оцінку відповідності. У 2025 році Мінцифри вже відхилило дві пропозиції від турецьких постачальників, які використовували підсистеми на основі китайських чіпів. Цей процес, хоча й повільний, поступово усуває технологічний хаос, що існував у попередні роки.

Особливу увагу заслуговує роль міжнародних фінансових інституцій. Світовий банк у 2024 році затвердив проєкт «Цифрове відновлення України» на суму 350 млн доларів США. У технічних вимогах до проєкту прямо зазначено: «Всі інформаційні системи повинні бути розгорнуті на інфраструктурі, що відповідає стандартам ЄС з кібербезпеки та захисту даних» [92]. Це фактично виключає участь компаній, які не мають сертифікації від ENISA або не дотримуються GDPR. Аналогічні умови включені в угоди з Міжнародним валютним фондом та Європейським інвестиційним банком. Таким чином,

навіть національні проєкти, фінансовані не з ЄС, тепер опосередковано підпадають під європейські правила.

Китайська сторона також адаптує свою стратегію. Замість прямих інвестицій, Пекін тепер акцентує увагу на непрямому впливі через треті країни. Наприклад, у 2025 році компанія Huawei відкрила представництво в Сербії, яке займається підтримкою проєктів у країнах Східної Європи, зокрема в Україні [20]. Сербія, не будучи членом ЄС, не підпадає під його регуляторні обмеження, тому може виступати платформою для надання послуг. Українські міста отримують пропозиції від сербських інтеграторів, які використовують китайські рішення, але формально не є пов'язаними з КНР. Це ускладнює регулювання та створює нові сірі зони.

У той же час, Україна має унікальні можливості використати свій досвід для участі в міжнародних ініціативах. У 2025 році Україна була запрошена до робочої групи ITU/3GPP з розробки стандартів для аварійного зв'язку в умовах війни [22]. Цей проєкт, співфінансований ЄС та США, передбачає створення резервних мереж на основі спутникових технологій та дронів. Українські розробники з Delta Telecom та AIS беруть участь у тестуванні, надаючи дані з реальних бойових умов. Така участь не тільки підвищує технологічний капітал країни, а й забезпечує доступ до передових рішень, які будуть стандартизовані на глобальному рівні.

Крім того, українські IT-компанії стають важливим елементом європейської стратегії. У 2024 році компанія GitLab Ukraine (колишній Evil Martians) була залучена до проєкту GAIA-X, де працює над модулями безпеки для децентралізованих хмар [61]. Це демонструє, що Україна може брати участь у формуванні європейської цифрової автономії не лише як реципієнт, а й як постачальник знань. Аналогічно, у 2025 році стартап Preply увійшов до європейського консорціуму з розробки етичних ШІ-моделей для освіти, фінансованого з Horizon Europe [34]. Такі проєкти створюють нові ланцюги кооперації, які не залежать від геополітичних розбіжностей.

Одним із ключових факторів, що визначає майбутнє української цифрової політики, є здатність до інституційного навчання на основі міжнародного досвіду. У цьому контексті особливо важливою є аналітична рефлексія щодо практик ЄС та КНР не як альтернативних моделей, а як систем управління технологічними ризиками. Україна має можливість уникнути стратегічних помилок, властивих обом полюсам: надмірної бюрократизації регуляторних процесів у ЄС та тотального державного контролю в КНР [77]. Замість імітації цілісних моделей, доцільною є селективна інтеграція окремих інструментів, адаптованих до національного контексту.

Конкретним прикладом такого підходу може стати розробка національного «Інструментарію цифрової безпеки», аналогічного європейському 5G Toolbox, але з урахуванням специфіки військово-політичної ситуації [81]. Такий інструментарій мав би передбачати чотири рівні оцінки постачальників:

- ✓ високий ризик – компанії, пов’язані з державними структурами країн, що не є членами Вассенаарської угоди;
- ✓ середній ризик – постачальники з непрозорою власністю або з історією порушень кібербезпеки;
- ✓ низький ризик – компанії, що мають ENISA- або ISO/IEC 27001-сертифікацію;
- ✓ стратегічні партнери – постачальники, які залучені до спільних досліджень з українськими інститутами та відповідають вимогам IT-безпеки НАТО.

Такий підхід дозволить запровадити гнучкий, але чітко структурований механізм управління постачаннями, який не буде базуватися на політичних преференціях, а на технічній оцінці.

Додатковим рівнем захисту має стати створення Національного реєстру довіри (National Trust Registry), який би акредитував іноземні компоненти, що використовуються у державних інформаційних системах [84]. Цей реєстр мав би функціонувати за принципом «чорного – сірого – білого списку»:

– чорний список – обладнання, заборонене до використання (наприклад, продукція Hikvision, Dahua, Huawei у критичній інфраструктурі);

– сірий список – технології, що можуть використовуватися лише після проходження аудиту з боку Держспецзв'язку та СБУ (наприклад, IoT-пристрої в громадських установах);

– білий список – постачальники, які вже пройшли верифікацію на рівні ЄС або НАТО і можуть використовуватися без додаткових процедур.

Цей механізм мав би бути інтегрований із європейською системою CyCLONe та ENISA Early Warning System, що забезпечить автоматичну синхронізацію з оновленнями щодо кіберзагроз.

Важливим елементом стратегії має стати розвиток власного сектору кібербезпеки. На сьогодні критична інфраструктура України залежить від імпортних рішень, що створює системний ризик. Незважаючи на успіхи українських розробників у сфері кіберзахисту (наприклад, компанії CloudDefense, HiddenLayer, Cyber Unit), вони не мають доступу до державних тендерів через відсутність сертифікації. У 2025 році Мінцифри започаткувало пілотний проєкт «Кібербезпека Made in Ukraine», спрямований на акредитацію національних рішень за стандартами ENISA. Перші результати показали, що українські системи виявлення вторгнень (IDS) та системи управління ідентифікацією (IAM) відповідають базовим європейським вимогам. Державна підтримка такого сектору – через преференції у закупівлях, фінансування R&D та інтеграцію в міжнародні проєкти – дозволить знизити зовнішню залежність і створити національну технологічну автономію у сфері безпеки.

Особливу увагу слід приділити цифровій освіті та професійному розвитку. Відповідно до дослідження Єврокомісії «Digital Skills in Ukraine 2025», у країні існує дефіцит понад 50 тис. фахівців у сфері кібербезпеки, стандартизації даних та аудиту ШІ-систем. Для усунення цього дефіциту необхідно інтегрувати європейські освітні стандарти (наприклад, ENISA Cybersecurity Training Framework) в українські вищі навчальні заклади. У 2024–2025 роках подібну роботу було розпочато у Національному технічному

університеті «КПІ» та Харківському національному університеті імені В. Н. Каразіна, де запроваджено магістерські програми з «Кібербезпеки критичної інфраструктури» та «Цифрової та інформаційної безпеки». Такі ініціативи мають бути розширені на регіональні університети та підтримані через спільні гранти з Horizon Europe.

Паралельно важливою є робота з місцевими органами влади. Саме на рівні громад найчастіше відбуваються закупівлі китайських технологій через неусвідомлення ризиків. У 2025 році Мінцифри запровадило обов'язковий курс «Цифрова безпека для місцевого управління», який проходять усі керівники департаментів цифрового розвитку. Проте навчання має бути поєднане з технічною підтримкою: створенням єдиного порталу технічної експертизи, куди міста зможуть надсилати пропозиції постачальників для безкоштовного аналізу. Такий підхід дозволить уникнути ситуацій, подібних до випадку зі школами в Києві, де обладнання ZTE було встановлене без технічної перевірки.

Крім того, Україна має використати свій унікальний досвід війни для участі в формуванні глобальних цифрових стандартів. Відомо, що з початку повномасштабного вторгнення українські оператори зв'язку та кіберпідрозділи зібрали унікальні дані щодо тактик ворожих DDoS-атак, маніпуляцій через фейкові мережі та поширення дезінформації. Ці дані є цінним джерелом для розробки систем раннього попередження. Участь українських експертів у робочих групах ITU, 3GPP та ETSI не лише підвищує технологічну репутацію країни, але й забезпечує вплив на визначення майбутніх норм. Наприклад, у 2025 році проєкт стандартизації систем «зв'язку в умовах повного обстрілу» було внесено до робочої програми ITU на пропозицію України разом із Польщею та Фінляндією. Такі ініціативи демонструють, що Україна може бути не просто споживачем технологій, а їхнім законодавцем у специфічних умовах.

Стратегічний шлях України має ґрунтуватися на чотирьох стовпах: інституційному регулюванні, розвитку власного кіберсектору, підвищенні компетентності кадрів та активній міжнародній стандартизації. Це дозволить країні збалансувати технологічну вразливість із можливостями глобальної

інтеграції, забезпечуючи при цьому національну безпеку, суверенітет даних та швидку цифрову модернізацію в умовах війни та відновлення.

Таким чином, Україна опиняється в унікальному положенні: вона змушена вибирати між моделями, але водночас має можливість формувати власний шлях. Ключовим фактором успіху стане здатність забезпечити інституційну зрілість: чітке регулювання, незалежний аудит, гармонізацію з європейськими стандартами. Без цього навіть найкращі наміри залишаться нереалізованими, а технологічна залежність перетвориться на стратегічну вразливість. Наразі Україна рухається у правильному напрямку, але темпи адаптації повинні прискоритися, щоб не відстати від глобальних змін, які визначають майбутнє цифрового світу.

Висновки до розділу 3

Аналіз проблем та перспектив інформаційно-цифрового партнерства між Китайською Народною Республікою та Європейським Союзом дозволяє зробити ряд узагальнюючих висновків щодо стану, динаміки та наслідків цієї взаємодії.

Цифрова сфера перетворилася на один із ключових арен стратегічного суперництва між КНР та ЄС. Це суперництво не є тимчасовим явищем, зумовленим окремими інцидентами, а відображає глибоку, структурну несумісність двох моделей організації цифрового простору. Для ЄС цифрові технології – інструмент реалізації прав людини, захисту приватності та демократичного управління. Для КНР – засіб забезпечення соціальної стабільності, державного контролю та технологічної автономії. Ця розбіжність проявляється у всіх ключових напрямах: кібербезпеці, штучному інтелекті, регулюванні даних, стандартизації. Тому конвергенція стандартів, навіть у технічних сферах, залишається малоймовірною.

Незважаючи на гостру конкуренцію, повна ізоляція між сторонами не відбувається. Замість цього формується модель «вибіркової, технічно обмеженої співпраці» у нішах, де взаємна вигода переважає над

геополітичними ризиками. Такі сфери включають фундаментальні дослідження без чутливих даних, стандартизацію енергоефективності, обмін підписами шкідливого ПЗ, підтримку цифрового розвитку третіх країн у гуманітарній сфері. Ці канали не мають на меті подолання стратегічної недовіри, але вони запобігають ескалації і зберігають мінімальний рівень взаємодії. Для ЄС такий підхід втілюється через концепції «відкритої стратегічної автономії» та «зменшення ризиків», для КНР – через «цифровий суверенітет» як інструмент контролю.

Крім того, ця конкуренція має прямі та вимірювані наслідки для України. З одного боку, вона створює технологічну дилему: китайські пропозиції часто є дешевшими і доступнішими, але їх використання загрожує втратою сумісності з європейською цифровою екосистемою. Це вже проявилося в реальних інцидентах – від замороження єврофінансування проєктів до виявлення китайського обладнання у критичній інфраструктурі через треті країни. З іншого боку, конкуренція відкриває можливості для України – отримання кращих умов від ЄС, участь у спільних проєктах з «зелених» технологій, інтеграція українських ІТ-компаній у європейські консорціуми.

Стратегічним викликом для України є відсутність єдиного регуляторного підходу до оцінки цифрових технологій. На відміну від ЄС, який має чіткі інструменти (Інструментарій 5G, AI Act, NIS2), Україна досі не створила механізму перевірки постачальників обладнання. Це дозволяє китайським компонентам потрапляти до державних систем через благодійні фонди, треті країни або неформальні угоди. У воєнних умовах ця вразливість перетворюється на загрозу національній безпеці.

Українська відповідь на ці виклики повинна ґрунтуватися на диференційованому підході. У критичних секторах – повна інтеграція з європейською нормативною системою. У соціальних сферах – обмежене використання нейтральних рішень за умови локалізації даних та незалежного аудиту. У науці та інноваціях – участь у міжнародних проєктах, які не мають

подвійного призначення. Такий підхід дозволяє уникнути бінарного вибору між ЄС і КНР і формує основу для власної цифрової державності.

У цілому, інформаційно-цифрове партнерство КНР–ЄС більше не є питанням технічної кооперації. Воно є відображенням більш широкого геополітичного розколу, у якому Україна виступає не просто спостерігачем, а активним учасником, чий вибір технологій визначатиме майбутнє її суверенітету, безпеки та євроінтеграції. У цих умовах ключовим завданням стає не пошук ідеального партнера, а раціональне управління взаємодією з обома великими державами – через чітке регулювання, інституційну зрілість і стратегічну прозорість.

ВИСНОВКИ

За результатами дослідження «Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційно-цифровому вимірі» можна зробити такі висновки:

1. Встановлено основні підходи до трактування міжнародної цифрової взаємодії, що дозволило визначити її як комплексну форму міждержавної комунікації, у якій технологічні, політичні та економічні елементи поєднуються у єдиному просторі прийняття рішень. Це, своєю чергою, забезпечило можливість охарактеризувати міжнародну цифрову взаємодію як новий вимір глобальної політики, у межах якого формуються механізми впливу через дані, інфраструктуру та технологічні стандарти, що визначають конфігурацію сил у світовій системі. Установлено, що прискорення цифрових процесів сприяє швидшому поширенню політичних сигналів та рішень, що змінює традиційні дипломатичні канали та посилює роль цифрових платформ. Саме їхнє формування створює передумови для появи нових суб'єктів впливу, здатних конкурувати з державами у питаннях регулювання технологічного розвитку та контролю над інформаційними потоками, що розширює коло учасників глобальної взаємодії. Прагнення держав закріпити власні цифрові стандарти як універсальні сформувало нормативне суперництво, у межах якого визначення правил доступу до даних стає інструментом політичного впливу.

2. Розкрито етапи становлення та розвитку цифрового партнерства між Китаєм та Європейським Союзом, яке еволюціонувало від технічної співпраці та обміну досвідом до інституційно оформленого, але суперечливого формату взаємодії. Постійне зміщення акцентів у взаєминах було зумовлене посиленням стратегічної конкуренції, нормативних розбіжностей і геополітичного контексту, що спричинило трансформацію партнерства у напрямі керованого суперництва, де співпраця зберігається лише у вибіркових технологічних сферах. Первинна орієнтація на економічну модернізацію поступово поступилася прагненню сторін формувати власні цифрові моделі, що

вплинуло на структуру взаємодії. Інституціоналізація співпраці через формати діалогу створила механізми координації політик, однак водночас підкреслила розбіжності у підходах до регулювання цифрової сфери. Розвиток політики цифрової автономії Європейського Союзу обмежив доступ Китаю до європейського ринку даних, що посилило нерівність у можливостях сторін. У відповідь Китай активізував поширення власних технологічних рішень та інфраструктури, зміцнюючи свою присутність на глобальному рівні. Це сприяло формуванню політики деризикування з боку Європейського Союзу, спрямованої на зменшення залежності від китайських технологій. Розбіжність інтересів визначила вибірковий характер співпраці, що зберігається лише там, де взаємодія є стратегічно доцільною. Така конфігурація призвела до появи моделі, у якій партнерство співіснує з конкуренцією та регуляторними обмеженнями, створюючи нестійкість цифрових взаємин.

3. Визначено ключові напрями цифрової взаємодії між сторонами, що включають співпрацю у сфері штучного інтелекту, кібербезпеки, цифрової інфраструктури, обігу даних і технологічної стандартизації. Їх розвиток демонструє прагнення сторін впливати на глобальні технологічні правила, формуючи власні моделі цифрового порядку, що зумовлює конкуренцію за домінування у стратегічних галузях. Подальше розширення співпраці у цих напрямках визначає здатність держав встановлювати технологічні вимоги, які матимуть міжнародне застосування, що поступово перетворює цифровий простір на сферу стратегічного суперництва. Розбудова цифрової інфраструктури створює основу для контролю над потоками даних, що посилює вплив сторін у глобальному вимірі. Формування стандартів у сфері штучного інтелекту стає інструментом визначення етичних, правових і технічних рамок, що впливатимуть на розвиток технологій у майбутньому. Спільні ініціативи у сфері кібербезпеки сприяють зміцненню довіри, однак зберігають залежність від політичних рішень, які можуть обмежувати співпрацю. Взаємодія щодо цифрової інфраструктури демонструє прагнення сторін створити власні мережеві екосистеми, що формують додаткові

можливості для поширення впливу. Контроль над обігом даних надає державам інструменти регулювання доступу до інформаційних ресурсів і створює умови для встановлення пріоритетності власних технологічних рішень.

4. Виокремлено основні виклики та ризики інформаційно-цифрової взаємодії, серед яких інституційна асиметрія, регуляторна несумісність, питання кібербезпеки, технологічна залежність та геополітичне протистояння. Сукупність цих чинників обмежує можливості для поглиблення співпраці та сприяє формуванню політики деризикування і селективної взаємодії, що свідчить про структурну нестабільність партнерства. Інституційна асиметрія ускладнює узгодження підходів, оскільки сторони мають різні моделі управління цифровою сферою та різний ступінь централізації прийняття рішень. Регуляторна несумісність створює бар'єри для інтеграції цифрових систем, що зменшує ефективність спільних проєктів і уповільнює їх впровадження. Технологічна залежність формує ризики втрати контролю над критично важливими інфраструктурними елементами, що посилює занепокоєння щодо безпеки. Питання кібербезпеки визначає можливість виникнення загроз, здатних вплинути на політичну стабільність і порушити функціонування цифрових мереж. Геополітичне протистояння додає додатковий вимір напруженості, оскільки цифрова сфера стає інструментом впливу у ширших міжнародних відносинах. Реакцією на ці ризики стає впровадження обмежувальних механізмів і посилення контролю за технологічними потоками, що звужує простір для співпраці. Політика деризикування спрямована на зменшення залежності від зовнішніх технологічних рішень, що формує вибірковість у взаємодії.

5. Визначено перспективи розвитку цифрового партнерства та його вплив на третіх акторів, насамперед Україну. Поєднання європейських нормативних стандартів і китайських технологічних рішень створює для України одночасно можливості модернізації цифрової інфраструктури та ризики зростання залежності від зовнішніх технологічних центрів. Це підкреслює необхідність формування збалансованої цифрової стратегії,

орієнтованої на інтеграцію до європейського цифрового простору та розвиток власної технологічної спроможності. Урахування європейських регуляторних підходів дозволяє Україні зміцнити правове поле у сфері захисту даних та забезпечити відповідність вимогам спільного ринку, що створює умови для розширення економічної взаємодії. Водночас наявність китайських технологічних пропозицій забезпечує доступ до інфраструктурних рішень і швидких технологічних модернізацій, що є важливим у контексті відновлення та розвитку цифрових систем. Така подвійність можливостей і загроз зумовлює потребу у стратегічному виборі, який визначатиме напрям інтеграції України в глобальний цифровий простір. Вибір моделі взаємодії впливає на рівень технологічної автономії держави та її здатність впроваджувати власні цифрові продукти й стандарти. Формування національної цифрової політики, що ґрунтується на європейських принципах і водночас враховує потенціал зовнішніх партнерів, сприятиме зміцненню конкурентоспроможності України. Збереження балансу між зовнішніми впливами є ключовим для уникнення надмірної залежності, яка може обмежити стратегічні рішення у сфері цифрового розвитку.

Інформаційно-цифрове партнерство між Китаєм та Європейським Союзом сформувалося як складний та багатовимірний формат взаємодії, у межах якого співпраця поєднується зі стратегічним суперництвом. Сукупність політичних, нормативних та технологічних чинників зумовлює нестійкість та вибірковість взаємин, що проявляється у різній глибині взаємодії за окремими напрямами. Така конфігурація сприяє формуванню нового цифрового порядку, де технології, дані та інфраструктура стають ключовими ресурсами впливу на глобальному рівні. Це, своєю чергою, визначає посилення конкуренції за технологічне лідерство та контроль над цифровими потоками, що впливає на баланс сил у міжнародній системі. За цих умов роль України набуває особливого значення, оскільки її залучення до європейського цифрового простору створює можливості для модернізації, водночас потребуючи стратегічного вибору та формування власної цифрової політики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2030 Digital Decade – Report on the state of the Digital Decade 2023. Europran Comission. URL: https://surl.li/zknzum (дата звернення: 17.10.2025).

2. 5G Trial Cooperation Between EU and China / A. Kostopoulos et al. 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019. 2019. https://doi.org/10.1109/iccw.2019.8756985

3. 5G Trial Cooperation Between EU and China / A. Kostopoulos et al. 2019 IEEE International Conference on Communications Workshops (ICC Workshops), *Shanghai*, *China,* 20–24 May 2019. 2019. https://doi.org/10.1109/iccw.2019.8756985

4. Ai M., Wang P., Bu Y. Climate policy and inclusive green growth: The role of China's low-carbon city pilot policy. *Journal of Cleaner Production.* 2025. Vol. 519. P. 145959. https://doi.org/10.1016/j.jclepro.2025.145959

5. Ai G. Asian Comparative Constitutional Law: Constitutional Amendments. *Asia Pacific Law Review*. 2025. P. 1–5. https://doi.org/10.1080/10192557.2025.2556088

6. Analysis of Economic and Trade Relations between China and the EU–Taking the China-EU Comprehensive Agreement on Investment as a Perspective. *Academic Journal of Business & Management.* 2021. Vol. 3, no. 8. https://doi.org/10.25236/ajbm.2021.030819

7. Antikainen M., Härkönen H. Artificial Intelligence and EU Design Law. *SSRN Electronic Journal.* 2023. https://doi.org/10.2139/ssrn.4575982

8. Apak S., Atay E. Global Competitiveness in the EU Through Green Innovation Technologies and Knowledge Production. *Procedia – Social and Behavioral Sciences.* 2015. Vol. 181. P. 207–217. https://doi.org/10.1016/j.sbspro.2015.04.882

9. Arendsen R. Towards Digital Transformation of EU-Customs?. *Global Trade and Customs Journal*. 2024. Vol. 19, Issue 6. P. 403–412. https://doi.org/10.54648/gtcj2024047

10. Arnold Z., Luong N. China's Artificial Intelligence Industry Alliance. Center for Security and Emerging Technology, 2021. https://doi.org/10.51593/20200094

11. Borges de Castro R. EU-China: 50 years without fireworks. URL: https://www.epc.eu/publication/eu-china-50-years-without-fireworks/ (date of access: 02.10.2025).

12. Bradford A. The Chinese State-Driven Regulatory Model'. *New York :* New York, 2023. https://doi.org/10.1093/oso/9780197649268.003.0003

13. Brinza A, Bērziņa-Čerenkova UA, Le Corre P, Seaman J, Turcsányi R, Vladisavljev S. EU-China relations: De-risking or de-coupling– the future of the EU strategy towards China. Publications Office of the European Union. Belgium. URL: https://surl.li/hfyzvh (date of access: 2.11.2025).

14. Carrozza I. Discourse and Norms along China's Digital Silk Road. *Asia Policy.* 2025. Vol. 20, no. 2. P. 101–126. https://doi.org/10.1353/asp 2025.a960045

15. Casarini N. A European strategic "third way?" *The European Union between the traditional transatlantic alliance and the pull of the Chinese market. China International Strategy Review.* 2022. https://doi.org/10.1007/s42533-022-00095-1

16. Casarini N. Rising to the Challenge: Europe's Security Policy in East Asia amid US-China Rivalry. *The International Spectator*. 2020. Vol. 55, no. 1. P. 78–92. https://doi.org/10.1080/03932729.2020.1712133

17. Chen B., Chen J. China's Legal Practices Concerning Challenges of Artificial General Intelligence. *Laws*. 2024. Vol. 13, no. 5. P. 60. https://doi.org/10.3390/laws13050060

18. Chinese Digital Economy / M. Zhaoli et al. Springer Singapore Pte. Limited, 2022.

19. Christiansen T., Dorussen H., Kirchner E. J. Security Cooperation in EU-China Relations: Towards Convergence?. *European Foreign Affairs Review*. 2018. Vol. 23, Issue 3. P. 287–304. https://doi.org/10.54648/eerr2018027

20. CHUNG C.-p. China's Digital Silk Road. *East Asian Policy*. 2023. Vol. 15, no. 02. P. 123–137. https://doi.org/10.1142/s1793930523000168

21. Conclusion and Outlook:. *The EU-China Security Paradox*. 2022. P. 149–153.: https://doi.org/10.2307/j.ctv269fw09.17 Dahlman E., Parkvall S., Sköld J. 5G standardization. 5G/5G-Advanced. 2024. P. 7–27. https://doi.org/10.1016/b978-0-443-13173-8.00011-6

22. Digital Humanism – Putting people at the centre of the digital transformation (CSA). Horizon-europe.gouv.fr. URL: https://surl.li/haaqlg (дата звернення: 16.10.2025).

23. Du K., Cheng Y., Yao X. Environmental regulation, green technology innovation, and industrial structure upgrading: *The road to the green transformation of Chinese cities. Energy Economics.* 2021. Vol. 98. P. 105247. https://doi.org/10.1016/j.eneco.2021.105247

24. EPC. EU-China: 50 Years Without Fireworks. Brussels : European Policy Centre, 2025. URL: https://surl.li/nggdio (date of access: 02.10.2025).

25. EPC. EU-China: 50 Years Without Fireworks. Brussels : European Policy Centre, 2025. URL: https://surl.li/iradax (дата звернення: 02.10.2025).

26. EU trade relations with China. Trade and Economic Security. URL: https://surl.li/rxzyhm (date of access: 01.11.2025).

27. EU-China High-Level Economic and Trade Dialogue (HED). *European Commission – European Commission*. URL: https://surl.li/bgbudi (date of access: 05.11.2025).

28. EU-China Relations: Factsheet. The Diplomatic Service of the European Union | EEAS. 2023. URL: https://surl.lu/kdhtph (date of access: 08.10.2025).

29. EU-China Relations: Factsheet. The Diplomatic Service of the European Union. EEAS. URL: https://surl.li/ppmpzy (дата звернення: 08.10.2025).

30. EU-China: Commission and China hold second High-level Digital Dialogue. Brussels, 2023. URL: https://surl.li/gyzahi (date of access: 11.11.2025).

31. European Commission. EU Trade Policy towards China. 2024. URL: https://surl.li/gfeood (date of access: 08.10.2025).

32. European Commission. EU Trade Policy towards China. 2024. URL: https://surl.li/epgyto (дата звернення: 08.10.2025).

33. European Parliament Resolution of 19 May 2021 on Artificial intelligence in education, culture and the audiovisual sector – Wednesday, 19 May 2021. URL: https://surl.li/wykolq (дата звернення: 06.11.2025).

34. Evas T. The EU Artificial Intelligence Act:. Journal of AI Law and Regulation. 2024. Vol. 1, no. 1. P. 98–101. URL: https://doi.org/10.21552/aire/2024/1/11 (date of access: 5.11.2025).

35. Fang L., Fang J. The Construction and Significance of the China-Europe Digital Partnership. *China Watch*. 2024. Vol. 4. URL: https://surl.li/wndamb (date of access: 12.11.2025).

36. Farrell H., Newman A. L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security. 2019. Vol. 44, no. 1. P. 42–79. URL: https://doi.org/10.1162/isec_a_00351 (date of access: 6.11.2025).

37. Framing EU–China Trade Relations: A Content Analysis of UK Newspaper Coverage (2001–2021) / X. Zhao et al. *Journalism Studies*. 2023. P. 1–19. URL: https://doi.org/10.1080/1461670x.2023.2260497 (date of access: 17.11.2025).

38. Gabriel J., Schmelcher S. Three scenarios for EU-China relations 2025. *Futures*. 2018. Vol. 97. P. 26–34. URL: https://doi.org/10.1016/j.futures.2017.07.001 (date of access: 17.11.2025).

39. García-Herrero A., Vasselier A. Updating the EU's strategy on China: Co-existence while de-risking through partnerships. URL: https://surl.li/zdoyko (date of access: 02.10.2025).

40. García-Herrero A., Vasselier A. Updating the EU's strategy on China: Co-existence while de-risking through partnerships. URL: https://surl.li/kzyyjd (дата звернення: 02.10.2025).

41. GDPR. Data Protection and Data Transfers Law. 2023. https://doi.org/10.5040/9781526524812.schedule-001

42. Geeraerts G. The EU-China partnership: balancing between divergence and convergence. *Asia Europe Journal*. 2019. Vol. 17, no. 3. P. 281–294. https://doi.org/10.1007/s10308-019-00554-2

43. Gemueva K. Huawei in EU Countries: Participation in the Development of 5G Networks. *Scientific and Analytical Herald of IE RAS*. 2020. Vol. 15, no. 3. P. 75–81. https://doi.org/10.15211/vestnikieran320207581

44. Gill B. Managing tensions and promoting cooperation: US–Europe approaches on security issues with China. *US-China-EU Relations. London,* 2010. P. 259–282. https://doi.org/10.4324/9780203860205-24

45. Godement F., Fox J. A Power Audit of EU-China Relations. 2009. URL: https://surl.li/jygtat (date of access: 05.11.2025).

46. Green technology innovation development in China in 1990–2015 / Q. Wang et al. *Science of The Total Environment*. 2019. Vol. 696. P. 134008. https://doi.org/10.1016/j.scitotenv.2019.134008

47. Gurol J. Conclusion and Outlook: The EU and China at a Crossroads. *The EU-China Security Paradox*. 2022. P. 149–153. https://doi.org/10.1332/policypress/9781529219630.003.0010

48. Harasimiuk D. E., Braun T. EU Policy Making in the AI Field. Regulating Artificial Intelligence. 2021. P. 15–47. https://doi.org/10.4324/9781003134725-3-3

49. Hill C., Smith Michael, Vanhoonacker-Kormoss, S. International Relations and the European Union. 3 ed. *Oxford University Press*, 2017. 600 p. https://doi.org/10.1093/hepl/9780198737322.001.0001

50. International cooperation with China in research and innovation. *European Commission*. URL: https://surl.li/nopvjw (date of access: 05.11.2025).

51. Keßler C. Between competition and co-operation: *How to engage with China on climate.* 2024. P. 3–11. URL: https://surl.li/abepjw (date of access: 08.10.2025).

52. Keßler C. Between competition and co-operation: How to engage with China on climate. 2024. P. 3–11.

53. KEUKELEIRE S. European Union Foreign Policy in a Changing World - By K.E. Smith. JCMS: Journal of Common Market Studies. 2009. Vol. 47, no. 4. P. 919–920. https://doi.org/10.1111/j.1468-5965.2009.02026_1.x

54. Lee G. China's Artificial Intelligence Education Policy. *Korea Digital Publishing Society*. 2025. Vol. 19. P. 41–59. https://doi.org/10.30580/kdips.2025.19.3.41

55. Levy K., Révész Á. No Common Ground: A Spatial-Relational Analysis of EU-China Relations. *Journal of Chinese Political Science*. 2021. https://doi.org/10.1007/s11366-021-09769-w

56. Li Z., Wang X., Zhang T. China Mobile in Action. 5G+. *Singapore,* 2020. P. 201–213. https://doi.org/10.1007/978-981-15-6819-0_14

57. Li Y., He Z. The Remaking of China–EUrope Relations in the New Era of US–China Antagonism. *Journal of Chinese Political Science*. 2022. https://doi.org/10.1007/s11366-022-09792-5

58. Liu H.-W., Zhou W. Digital regulation in the shadow of digital empires: a quest for cooperation?. *Journal of International Economic Law.* 2024. https://doi.org/10.1093/jiel/jgae002

59. Loidl V. Transatlantic cooperation and the digital economy: *The impact of the new strategic agenda "a Europe fit for the digital age"*. Illinois, 7 October 2025. 2020. P. 25–60. URL: https://hdl.handle.net/2142/108529 (date of access: 23.10.2025).

60. Ma H., Haq D. M. Z. The European Union's Digital Sovereignty Protection Model in the Big Data Era. *Advances in Information Management and Economic Development Research.* 2025. Vol. 2, no. 1. P. 168. https://doi.org/10.70114/aimedr.2025.2.1.p168

61. Manners I. Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies.* 2002. Vol. 40, no. 2. P. 235–258. https://doi.org/10.1111/1468-5965.00353

62. Marcus J. S. Digital aspects of the eu single market. 2024. 52 p. URL: https://surl.li/pfwgiw (date of access: 06.10.2025).

63. Marcus J. S. Digital aspects of the EU single market. 2024. 52 p. URL: https://surl.li/jijxat (дата звернення: 06.10.2025).

64. Melnychuk V. From partnership to rivalry: the role of ideological and security differences in eu-china relations. Філософія та політологія в контексті сучасної культури. 2025. Vol. 17, no. 1. P. 241–247. https://doi.org/10.15421/352531

65. Moore G.J. Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies. *J OF CHIN POLIT SCI* 28, 2023. 151–167. https://doi.org/10.1007/s11366-022-09814-2

66. Nalbantoglu C. EU – China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace. *Cuadernos Europeos de Deusto*. 2022. No. 05. P. 51–73. URL: https://doi.org/10.18543/ced.2555 (date of access: 5.11.2025).

67. Niu J. The Sovereignty Exception: China's State-Centric Approach to National Security in Cross-Border Data Flows. Lecture *Notes in Education Psychology and Public Media*. 2025. №107. P. 60-66. https://doi.org/10.54254/2753-7048/2025.LD27192

68. Okano-Heijmans M., Vosse W. Promoting open and inclusive connectivity: The case for digital development cooperation. *Research in Globalization*. 2021. Vol. 3. P. 100061. https://doi.org/10.1016/j.resglo.2021.100061

69. Petry J. China's rise, weaponised interdependence and the increasingly contested geographies of global finance. *Finance and Space.* 2024. Vol. 1, no. 1. P. 49–57. https://doi.org/10.1080/2833115x.2023.2296439

70. Politi A. The paradigm-shift in eu-china relations and the limits of the eu's current strategy towards china: a relational perspective. *Asian Affairs*. 2023. P. 1–24. https://doi.org/10.1080/03068374.2023.2281164

71. Prokopyshyn O., Trushkina N. The geopolitics of cybersecurity: a comparative analysis of national strategies for digital sovereignty. *Politics & Security.* 2025. Vol. 12, no. 2. P. 59–71. URL: https://doi.org/10.54658/ps.28153324.2025.12.2

72. Qin G. Building on Past Successes and Bringing China-EU Relations to New Heights under the New Situation. 中国人民外交学会官网. URL: https://www.cpifa.org/en/cms/book/312 (date of access: 17.11.2025).

73. Sahakyan M. D. China's digital silk road and the eurasian economic union's member states: cooperation, challenges, and opportunities. *Asian Affairs*. 2024. P. 1–20. https://doi.org/10.1080/03068374.2024.2421501

74. Santaniello M. Attributes of Digital Sovereignty: A Conceptual Framework. *Geopolitics.* 2025. P. 1–22. https://doi.org/10.1080/14650045.2025.2521548

75. Science E. Response to the European Commission's Inception Impact Assessment on Artificial Intelligence. 2020. https://doi.org/10.5281/zenodo.4916186

76. Securing Europe's competitiveness: Addressing its technology gap / S. Smit et al. McKinsey & Company. URL: https://surl.li/iaidpn (date of access: 03.10.2025).

77. State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU\'s digital transformation by 2030. European Commission – European Commission. URL: https://surl.lu/mfdzgu (date of access: 07.10.2025).

78. Study on Challenges and Countermeasures for Deepening Scientific and Technological Innovation Cooperation under the Framework of China-EU "*Belt and*

Road Initiative" Cooperation. JIS 2025, 3 (3), 1-7. https://doi.org/10.5281/zenodo.17232600

79. Su R., Liu H. Cautious optimism: unravelling Chinese views on European strategic autonomy. *Journal of European Integration*. 2025. Vol. 47, no. 6. P. 865–883. https://doi.org/10.1080/07036337.2025.2537373

80. Su R., Zhang D. Adaptive Sovereignty: China's Evolving Legislative *Framework for Transnational Data Governance.* 2025. https://doi.org/10.17645/pag.10413

81. Suetyi L., Yijia H., Xinxin C. Resilient partnership? EU perception and expectation from China. *Journal of Contemporary European Studies.* 2025. P. 1–17. https://doi.org/10.1080/14782804.2025.2500390

82. Taylor M. R. Inside the EU–China Human Rights Dialogue: assessing the practical delivery of the EU's normative power in a hostile environment. *Journal of European Integration.* 2020. P. 1–16. https://doi.org/10.1080/07036337.2020.1854245

83. Taylor M. R. Inside the EU–China Human Rights Dialogue: assessing the practical delivery of the EU's normative power in a hostile environment. *Journal of European Integration.* 2020. P. 1–16. https://doi.org/10.1080/07036337.2020.1854245

84. The International Digital Strategy for the European Union. Shaping Europe's digital future. URL: https://surl.li/tidzfz (дата звернення: 18.10.2025).

85. Tovkun L. V., Leonovych M. Y. Legal regulation of artificial intelligence: international experience and prospects for implementation in ukraine. *Juridical scientific and electronic journal.* 2024. No. 12. P. 278–282. https://doi.org/10.32782/2524-0374/2024-12/62

86. Ulrich J. EU-China relations in challenging times. 2021. P. 3–11. URL: https://surl.li/fkczsw (date of access: 03.11.2025).

87. Valeriano B. The Correlates of Cyber Strategy. *Oxford University Press*, 2018. https://doi.org/10.1093/oso/9780190618094.003.0003

88. Vernon J. State of artificial intelligence in Europe. *HiPEAC Vision 2024*. 2024. Rationale. https://doi.org/10.5281/zenodo.10874814

89. VIRGEBAU K. EU-CHINA relations. 17/2021 L'EUROPE UNIE / UNITED EUROPE, PARIS, No-17/2021, Print ISSN: 2780-8173, On line ISSN: 2743-4052 Linking ISSN (ISSN-L): 2743-4052 EAN: 99782749700519 https://doi.org/10.5281/zenodo.15534012

90. Wagner C. S., Simon D. F. China's use of formal science and technology agreements as a tool of diplomacy. *Science and Public Policy*. 2023. URL: https://doi.org/10.1093/scipol/scad022 (date of access: 17.11.2025).

91. What is GDPR, the EU's new data protection law? – GDPR.eu. GDPR.eu. URL: https://gdpr.eu/what-is-gdpr/ (date of access: 04.10.2025).

92. Wo S.. The U.S. is Back in the 5G Game. Wall Street Journal. 2021. URL: https://www.wsj.com/articles/us-5g-companies-11621870061 (дата звернення: 19.10.2025).

93. Wolf S. Charlotte Bretherton and John Vogler, The European Union as Global Actor (2006) – [Charlotte Bretherton and John Vogler, The European Union as Global Actor, (New York: Routledge, 2nd edition, 2006, ISBN: 0-415-28244-6)]. *German Law Journal.* 2008. Vol. 9, no. 2. P. 211–215. https://doi.org/10.1017/s2071832200006398

94. Wong R. The Issue of Identity in the EU-China Relationship. *Politique européenne.* 2013. Vol. 39, no. 1. P. 158. https://doi.org/10.3917/poeu.039.0158

95. Xia J. China 5G: Opportunities and Challenges. *Telecommunications Policy*. 2022. Vol. 46, no. 2. P. 102295. https://doi.org/10.1016/j.telpol.2021.102295

96. Yang X. Investment Value in China's Artificial Intelligence Industry. *BCP Business & Management*. 2022. Vol. 34. P. 1437–1443. https://doi.org/10.54691/bcpbm.v34i.3196

97. Zaidan E., Ibrahim I. A. AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanities and Social Sciences Communications.* 2024. T. 11, № 1. DOI: https://doi.org/10.1057/s41599-024-03560-x

98. Zeng J. China's Security Politics of AI. *Artificial Intelligence with Chinese Characteristics. Singapore,* 2022. P. 35–66. https://doi.org/10.1007/978-981-19-0722-7_3

99. Zeng J. China's Authoritarian Governance and AI. *Artificial Intelligence with Chinese Characteristics*. Singapore, 2022. P. 67–103. https://doi.org/10.1007/978-981-19-0722-7_4

100. Zhao B. A Design Model of English Auxiliary Teaching System Using Artificial Neural Networks. *Mobile Information Systems*. 2022. Vol. 2022. P. 1–11. https://doi.org/10.1155/2022/8694532

АНОТАЦІЯ

Кітаніна В.О. Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційно-цифровому вимірі (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 102 с. (рукопис).

Мета дослідження – з'ясувати сучасний стан та основні напрями розвитку інформаційно-цифрового партнерства між Китайською Народною Республікою та Європейським Союзом.

Об'єкт дослідження – відносини між Китайською Народною Республікою та Європейським Союзом в інформаційноцифровому вимірі.

Предмет дослідження – інформаційно-цифрове партнерства між Китайською Народною Республікою та Європейським Союзом.

У першому розділі розкрито теоретико-історичні засади інформаційних відносин між КНР та ЄС, охарактеризовано підходи до вивчення цифрової взаємодії, визначено особливості інформаційно-цифрового виміру міжнародних відносин та окреслено еволюцію політичного діалогу КНР–ЄС у царині цифрової співпраці протягом 1995–2025 рр.

У другому розділі представлено соціально-політичний та економічний профіль КНР і ЄС як акторів міжнародних відносин, досліджено цифрові політики обох сторін у сферах кібербезпеки, штучного інтелекту, цифрового суверенітету та технологічного регулювання, а також визначено основні інструменти та механізми інформаційно-цифрової взаємодії.

У третьому розділі окреслено ключові виклики та ризики розвитку цифрового партнерства КНР–ЄС, визначено перспективні напрями співпраці у стратегічно важливих технологічних сферах, а також розглянуто вплив інформаційно-цифрового виміру цих відносин на Україну з урахуванням можливостей модернізації цифрової інфраструктури та ризиків посилення зовнішніх залежностей.

Ключові слова: КНР–ЄС, інформаційно-цифрові відносини, цифровий суверенітет, кібербезпека, цифрове партнерство, технологічна політика.

ANNOTATION

Kitanina V. O. Relations between the People's Republic of China and the European Union in the Information-Digital Dimension (master's work). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 102 p. (manuscript).

The aim of the study is to clarify the current state and key directions of development of the information-digital partnership between the People's Republic of China and the European Union.

The object of the study is PRC–EU relations in the information-digital sphere.

The subject of the study is the information-digital partnership between the People's Republic of China and the European Union.

The first chapter reveals the theoretical and historical foundations of information relations between China and the EU, identifies key approaches to studying digital interaction, defines the main features of the information-digital dimension of international relations, and traces the evolution of PRC–EU political dialogue on digital cooperation from 1995 to 2025.

The second chapter presents the socio-political and economic profiles of China and the EU as actors in international relations, examines their respective digital policies in the areas of cybersecurity, artificial intelligence, digital sovereignty and technology regulation, and identifies the principal mechanisms and instruments of information-digital interaction.

The third chapter outlines the key challenges and risks affecting the development of the PRC–EU digital partnership, defines promising avenues for cooperation in strategically important technological domains, and examines the implications of the information-digital dimension of these relations for Ukraine, taking into account both the opportunities for modernising its digital infrastructure and the risks of increasing external dependencies.

Keywords: PRC–EU relations, information-digital relations, digital sovereignty, cybersecurity, digital partnership, technology policy.

ВІДГУК

керівника кваліфікаційної роботи магістра
2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Кітаніної Валерії Олександрівни
на тему «Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційно-цифровому вимірі»

Обрана тема є досить актуальною з огляду на стрімку трансформацію глобального цифрового середовища та зростання значення інформаційних технологій у міжнародних відносинах. Взаємодія між Китайською Народною Республікою та Європейським Союзом у цифровій сфері формується в умовах конкуренції технологічних моделей, переосмислення підходів до кібербезпеки, управління даними та розвитку штучного інтелекту. Дослідження інформаційно-цифрового виміру цих відносин є важливим для розуміння балансу інтересів, ризиків і можливостей, що виникають на перетині політичних, економічних та регуляторних процесів. Актуальність роботи підсилюється впливом цифрової політики ЄС на країни-партнери, зокрема Україну, та глобальними наслідками посилення технологічної конкуренції між провідними державами.

Кваліфікаційна робота вирізняється високим рівнем наукової культури, логічністю структури та ґрунтовністю опрацювання джерельної бази. Авторка продемонструвала вміння працювати з широким колом джерел: науковими публікаціями, аналітичними матеріалами європейських і китайських дослідницьких центрів, документами Європейської Комісії, нормативно-правовою базою КНР і ЄС.

Крім того, сильною стороною дослідження є ґрунтовне розкриття сутності інформаційно-цифрового виміру міжнародних відносин та його ключових компонентів: управління даними, кібербезпеки, цифрових платформ, регуляторної політики та технологічного суверенітету. Авторка послідовно окреслює еволюцію підходів Китайською Народною Республікою та Європейського Союзу до цифрової взаємодії, аналізує інструменти м’якої сили, цифрову дипломатію, економічні інтереси та нормативні моделі сторін.

У роботі висвітлено сучасні виклики двосторонньої взаємодії, зокрема питання залежності від технологічних платформ, конкуренцію у сфері штучного інтелекту, відмінності в регуляторних підходах та потенційні ризики для кібербезпеки. Стиль викладу характеризується ясністю формулювань, послідовністю думки та науковою виваженістю.

Результати дослідження мають прикладну цінність для аналітичних структур, органів державної влади, дипломатичних установ та освітніх програм. Сформульовані положення можуть бути використані для підготовки матеріалів, що стосуються цифрової дипломатії, формування міжнародної цифрової політики та вироблення позиції України у відносинах з Китайською Народною Республікою та Європейським Союзом.

Дослідження містить чіткі висновки щодо регуляторних підходів сторін, що може бути корисним у процесі адаптації українського законодавства до регуляторних рамок ЄС у цифровій сфері. Аналітичні напрацювання авторки становлять основу для подальших досліджень, присвячених питанням кібербезпеки, штучного інтелекту, цифрової інфраструктури та міжнародного співробітництва в цих галузях.

Недоліки роботи мають несуттєвий характер. Місцями спостерігається надмірна деталізація окремих теоретичних понять, що дещо уповільнює динаміку викладу. Окремі фрагменти могли б бути подані стисло, без втрати змістовної насиченості. Проте ці особливості не впливають на наукову цінність дослідження та не порушують його логічної цілісності.

Кваліфікаційна робота Кітаніної Валерії Олександрівни є змістовною, логічно впорядкованою та виконаною на високому академічному рівні. Робота відповідає усім вимогам, що висуваються до магістерських кваліфікаційних робіт, вирізняється науковою обґрунтованістю, чіткістю висновків та практичною спрямованістю. Авторка продемонструвала високий рівень професійної підготовки та здатність працювати зі складною зовнішньополітичною проблематикою.

Робота заслуговує на оцінку «відмінно», а здобувачка – на присвоєння кваліфікації магістра з міжнародних відносин, суспільних комунікацій та регіональних студій; міжнародної інформаційної безпеки.

Науковий керівник:
канд. екон. наук, доцент, доцент
кафедри міжнародних відносин
Харківського національного університету
імені В.Н. Каразіна Ірина ПАНОВА

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації
та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Кітаніної Валерії Олександрівни
на тему «Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційноцифровому вимірі»

Кваліфікаційна робота присвячена актуальній та надзвичайно важливій проблематиці, а саме: трансформації взаємин між КНР та ЄС в умовах цифровізації міжнародних відносин. Обрана тема є своєчасною з огляду на глобальне змагання технологічних моделей, зростання значення цифрового суверенітету та політизацію обігу даних. У вступі авторка коректно визначає мету, завдання, об'єкт і предмет дослідження, обґрунтовує актуальність теми і формує широку джерельну базу, що включає нормативні документи ЄС і КНР, аналітику міжнародних організацій та академічні праці. Структура роботи логічна та відповідає вимогам до магістерських кваліфікаційних досліджень.

У першому розділі авторка демонструє глибоку обізнаність із сучасним теоретичним дискурсом міжнародних відносин. Ґрунтовно висвітлено такі концепції, як цифровий суверенітет, цифрова геополітика, інформаційна взаємозалежність, системне тертя та неокласичний реалізм. Окреслено ключові підходи до вивчення єврокитайських відносин, подано розгорнутий огляд літератури й політичних документів, що є важливою сильною стороною роботи.

Другий розділ присвячений аналізу цифрової політики КНР і ЄС у сферах штучного інтелекту, кібербезпеки, регулювання даних та інфраструктури. Авторка коректно систематизує різні нормативні підходи, вміло інтегрує у виклад широке коло стратегічних документів та аналізує механізми взаємодії між сторонами.

У третьому розділі розглянуто виклики інформаційно-цифрової взаємодії та перспективи подальшого партнерства. Позитивно оцінюється увага до впливу єврокитайського цифрового суперництва на Україну, тобто питання, що має високу практичну значущість. Це ж впливає і на той факт, що робота вирізняється міждисциплінарним підходом, здатністю авторки систематизувати великий обсяг теоретичної інформації, широким використанням іноземних джерел та науково-аналітичних матеріалів. Це свідчить і про достатній рівень підготовки.

Крім того, сформульовані у роботі положення мають практичну спрямованість і можуть бути використані для вдосконалення підходів України до розбудови цифрового співробітництва з Європейським Союзом та Китайською Народною Республікою, а також для глибшого розуміння особливостей інформаційно-цифрової взаємодії між провідними глобальними акторами. Отримані висновки є обґрунтованими та повністю відповідають визначеним у вступі меті й завданням. Перелік використаних джерел є достатньо широким і включає значну кількість зарубіжних наукових і аналітичних матеріалів, що підкреслює наукову значущість теми та високий рівень опрацювання інформаційної бази.

Однак, з огляду на позитивні аспекти кваліфікаційної роботи, варто звернути увагу на певні дискусійні та критичні положення, які потребують уточнень, додаткових пояснень та подальшої роботи авторки.

По-перше, незважаючи на широку теоретичну базу, у роботі відчутний дефіцит авторських аналітичних інструментів, порівняльних критеріїв, показників чи моделей, адже брак емпіричних даних (статистики, графіків, метрик цифрової взаємодії) обмежує дослідницьку новизну.

По-друге, в тексті роботи авторка лише окреслює ключові напрями (5G, ШІ, кібербезпека), але не подає розгорнутих прикладів реалізації конкретних проєктів або наслідків співпраці для обох сторін, що не дозволяє повною мірою оцінити ефективність цифрового партнерства.

По-третє, у вступі підкреслено важливість теми для України, але: аналітика щодо ризиків та можливостей для України у розділі 3.3. досить загальна, а також немає детального аналізу участі України в DSR, торговельно-технологічних ланцюгах, 5G-інфраструктурі, кібербезпеці тощо.

Проте означені зауваження жодним чином не зменшують якість та актуальність кваліфікаційної роботи, а скоріше слугують потенційними візіями для подальшого розвитку обраної проблематики. Адже кваліфікаційна робота Кітаніної Валерії Олександрівни на тему «Відносини між Китайською Народною Республікою та Європейським Союзом в інформаційноцифровому вимірі» є самостійним, добре структурованим дослідженням, що демонструє високий рівень підготовки авторки, вміння працювати з великим масивом джерел і систематизувати складні концептуальні підходи. Вважаю, що Кітаніна Валерія Олександрівна заслуговує на позитивну оцінку та на присвоєння кваліфікації магістра з *міжнародних відносин*, суспільних комунікацій та регіональних студій; міжнародної інформаційної *безпеки*.

Рецензент:
доктор філософії (PhD) з політології,
доцент закладу вищої освіти
кафедри політичної соціології
ННІ соціології та медіакомунікацій
Харківського національного
Університету імені В.Н. Каразіна

Руслан ЗАПОРОЖЧЕНКО