DOI: 10.18372/2307-9061.78.21133
УДК 340.5:338.94(510:477)

С. Я. Лихова,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0003-4755-7474

П. Д. Біленчук,
кандидат юридичних наук, професор
ORCID ID: https://orcid.org/0000-0002-9599-0347

Т. В. Обіход,
кандидат фізико-математичних наук, старший науковий співробітник
ORCID ID: https://orcid.org/0000-0003-1103-4006

ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЧНОГО РОЗВИТКУ КИТАЮ ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

Державний університет «Київський авіаційний інститут»
проспект Любомира Гузара, 1, 03058, Київ, Україна
Європейська академія прав людини
Інститут ядерних досліджень НАН України
проспект Науки, 47, 03028, Київ, Україна
E-mails: k_kpipp@ukr.net, aur.consalt@gmail.com, obikhod@kinr.kiev.ua

Метою *статті є дослідження системи правового регулювання технологічного розвитку Китайської Народної Республіки в контексті реалізації 15-ї п'ятирічної програми (2026–2030) та розробка науково обґрунтованих рекомендацій для вдосконалення законодавства України у сфері технологічної безпеки.* ***Методи дослідження****: використано порівняльно-правовий аналіз, а також методи системного і функціонального підходів.* ***Результати****: проаналізовано ідеологічне підґрунтя концепції «виробничих сил нового якості», що отримала конституційний статус; досліджено трифазову модель правового регулювання технологій (дерегуляція → системне законодавство → глобальне лідерство); розкрито правову архітектуру регулювання штучного інтелекту, квантових технологій, нейроінтерфейсів та водневої енергетики; виявлено принцип «подвійного стандарту» для державних і приватних суб'єктів; розглянуто доктрину «цивільно-військового злиття» як ключовий правовий механізм подвійного використання технологій; встановлено, що КНР випередила ЄС у прийнятті секторальних актів з регулювання ШІ.* ***Обговорення****: сформульовано рекомендації для законодавчої та регуляторної політики України в технологічній сфері в умовах воєнного стану та євроінтеграційного курсу, зокрема: прийняття Закону про штучний інтелект на основі AI Act ЄС; запровадження квантово-стійкого шифрування за стандартами NIST; регулювання технологій подвійного використання через експортний контроль; створення Міжвідомчого центру технологічної безпеки; запровадження «регуляторних пісочниць»; ідентифіковано загрози для України, пов'язані з доктриною цивільно-військового злиття, квантовою загрозою «Q-Day» та технологічною залежністю через стандарти 6G і систему «Бейдоу».*

Ключові слова: *правове регулювання технологій; штучний інтелект; цивільно-військове злиття; квантові технології; 15-та п'ятирічна програма КНР; технологічна безпека; євроінтеграція; Україна.*

Постановка проблеми та її актуальність. Стрімка трансформація глобального технологічного порядку, що відбувається у 2020-х роках, кардинально змінює не лише економічний і військовий баланс сил, а й саму архітектуру міжнародного та національного права. Штучний інтелект, квантові технології, синтетична біологія та нові енергетичні системи перестали бути суто технічними явищами – вони перетворилися на об'єкти правового регулювання, предмет міжнародних суперечок і безпосередній чинник геополітичного суперництва [1, 2].

Китайська Народна Республіка (КНР) посідає особливе місце в цьому процесі. За рівнем законотворчої активності у сфері цифрових технологій та штучного інтелекту КНР перевершила всі інші держави: починаючи з 2022 року країна послідовно ухвалює секторальні нормативні акти, випереджаючи навіть Євросоюз, чий Акт про штучний інтелект (AI Act) набув чинності лише в серпні 2024 року [3, 4]. При цьому китайська правова модель принципово відрізняється від ліберально-демократичних підходів: вона поєднує ринкові стимули з партійно-ідеологічним контролем, цивільне регулювання – з оборонним плануванням.

Для України актуальність дослідження цієї моделі є багатовимірною. По-перше, країна, що перебуває у стані збройного конфлікту з Росією, яка стратегічно наближена до КНР, безпосередньо відчуває вплив китайських технологій у сфері безпілотних систем, засобів радіоелектронної боротьби та інформаційних операцій [5]. По-друге, Україна, рухаючись курсом євроінтеграції, змушена одночасно приводити своє законодавство у відповідність до стандартів ЄС і будувати власну систему технологічної безпеки. По-третє, хаотичне й несистемне регулювання нових технологій в Україні створює вразливості як для іноземного технологічного проникнення, так і для втрати конкурентоспроможності у постконфліктному відновленні [6].

Отже, аналіз китайської правової моделі регулювання технологій є не академічним завданням, а прикладною необхідністю для формування ефективної технологічної політики України.

Аналіз досліджень і публікацій з проблеми. Стрімка трансформація глобального технологічного порядку та поява нових форм правового регулювання технологій зумовили значний науковий інтерес до цієї проблематики. У вітчизняній правовій науці окремі аспекти технологічного розвитку досліджували П.Д. Біленчук, Т.В. Обіход, С.Я. Лихова, Н.І. Сватюк, Ю.С. Шемшученко та інші вчені, проте комплексного порівняльно-правового аналізу китайської моделі регулювання технологій у контексті 15-ї п'ятирічної програми КНР досі не проводилося.

У зарубіжній доктрині значний внесок у дослідження китайського підходу до регулювання штучного інтелекту зробили Г. Робертс, Дж. Коулз, Дж. Морлі, М. Таддео, В. Ван та Л. Флоріді, які проаналізували політичні, етичні та регуляторні аспекти розвитку ШІ (Штучний Інтелект) в Китаї. Питання квантових технологій та геополітичної конкуренції досліджували Е.Б. Каня та Дж. Костелло. Р. Кремерс зосередився на аналізі структури захисту даних у Китаї, тоді як А. Дафо розробив дослідницьку програму з управління штучним інтелектом.

Правові аспекти китайської оборонної економіки та інновацій досліджував Т.М. Чен, а Р. Кало заклав основи для розуміння політики у сфері штучного інтелекту. Колективна монографія під редакцією Г. Вебстер, Р. Кремерс, П. Тріоло та Е. Каня присвячена механізмам розробки та прийняття регуляторних рішень у сфері ШІ в Китаї.

Разом з тим, незважаючи на наявність численних публікацій з окремих аспектів китайського технологічного регулювання, залишається недостатньо дослідженим системний характер цієї правової моделі, її ідеологічне підґрунтя у вигляді концепції «виробничих сил нового якості», а також практичні наслідки доктрини цивільно-військового злиття для третіх країн, зокрема України. Відсутні також комплексні рекомендації щодо адаптації українського законодавства до викликів, що породжуються китайською технологічною стратегією в умовах воєнного стану та євроінтеграційного курсу.

Метою статті є комплексний порівняльно-правовий аналіз системи правового регулюван-

ня технологічного розвитку КНР та розробка науково обґрунтованих рекомендацій для вдосконалення законодавства України у сфері технологічної безпеки та регулювання нових технологій.

Для досягнення мети визначено такі завдання:

- розкрити ідеологічне і конституційно-правове підґрунтя технологічної стратегії КПК (Комуністична Партія Китаю), зокрема доктрину «виробничих сил нового якості»;
- проаналізувати трифазову модель правового регулювання технологій у КНР та виявити її відмінності від підходів ЄС і США;
- дослідити правові механізми реалізації доктрини цивільно-військового злиття та її вплив на міжнародне технологічне право;
- охарактеризувати секторальне законодавство КНР щодо штучного інтелекту, квантових технологій, нейроінтерфейсів і водневої енергетики;
- виявити загрози для безпеки України, що випливають із китайської технологічної стратегії;
- сформулювати конкретні пропозиції щодо вдосконалення законодавства та регуляторної політики України.

Методологічну основу статті становить комплекс загальнонаукових та спеціально-правових методів, вибір яких зумовлений міждисциплінарним характером предмета дослідження. Основним методом є порівняльно-правовий аналіз, що дозволяє зіставити нормативні конструкції і регуляторні моделі різних правових систем — китайської (соціалістичної правової сім'ї), континентальної (ЄС) та загального права (США). Порівняння здійснюється на трьох рівнях: по-перше, на рівні принципів і доктрин (наприклад, принцип «регулювання через ліцензування» у КНР проти «регулювання через оцінку ризику» в ЄС); по-друге, на рівні нормативних інструментів (законів, підзаконних актів, стандартів); по-третє, на рівні правозастосовної практики та інституційних механізмів контролю.

Системний метод застосовується для дослідження китайського технологічного законодавства як цілісної системи із взаємопов'язаними елементами, а не як сукупності розрізнених нормативних актів. Це дозволяє виявити системоутворювальні принципи (наприклад, принцип «подвійного стандарту» для державних і приватних суб'єктів), ієрархічні зв'язки між рівнями регулювання (конституційним, законодавчим, підзаконним, стандартизаційним) та функціональні залежності між цивільним і оборонним секторами.

Функціональний метод спрямований на виявлення реальних (а не задекларованих) функцій правових норм. Наприклад, аналіз «Тимчасових положень про генеративний ШІ» КНР демонструє, що поряд із задекларованою функцією забезпечення безпеки ці норми виконують функцію ліцензійного контролю доступу на ринок і функцію вбудовування цензурного механізму в технічну архітектуру систем. Саме функціональний аналіз дозволяє оцінити реальну ефективність правових інструментів і виявити прихованих бенефіціарів регулювання.

Формально-юридичний метод використовується для точного відтворення і тлумачення нормативних положень китайського, європейського та американського законодавства. Цей метод є особливо важливим при аналізі таких документів, як правила розпізнавання облич 2024 року, де буквальне тлумачення норм дозволяє виявити законодавчо закріплений «принцип подвійного стандарту».

Виклад основного матеріалу дослідження. Центральна проблема, яку досліджує ця стаття, формулюється таким чином: чи є китайська система правового регулювання технологій цілісною і свідомо сконструйованою моделлю, що забезпечує конкурентні переваги в умовах глобального технологічного суперництва, — і якщо так, які її елементи становлять загрозу для України, а які можуть бути адаптовані до її правової системи?

Дослідження відповідає на такі конкретні питання:

Яким чином ідеологічна доктрина КПК трансформується у правові зобов'язання у сфері технологічного розвитку?

Яку роль відіграє доктрина цивільно-військового злиття у формуванні правової ар-

хітектури технологічного сектора КНР і які правові наслідки вона має для третіх країн?

Чому Китай обрав послідовну (а не превентивну) модель регулювання технологій і в чому її переваги та вади порівняно з підходами ЄС?

Які конкретні законодавчі та регуляторні заходи потребує Україна для захисту від технологічних загроз і використання відкритих можливостей?

Відповідь на ці питання вимагає аналізу первинних нормативних джерел КНР (законів, стандартів, урядових програм), порівняльного дослідження підходів ЄС і США, а також оцінки наявного стану законодавства України у відповідних сферах. Слід наголосити, що дослідження свідомо не розглядає питання, пов'язані із застосуванням технологій штучного інтелекту як таких: стаття зосереджена виключно на правовому вимірі технологічного розвитку — нормотворчих механізмах, регуляторних моделях і правовій архітектурі.

Технологічна стратегія Китайської Народної Республіки на сучасному етапі є невіддільною від ідеологічної конструкції Комуністичної партії Китаю. Концепція «виробничих сил нового якості», офіційно проголошена Сі Цзіньпіном у 2023 році та вписана до доктрини «економічних ідей Сі Цзіньпіна», є не просто економічною програмою, а правовим і партійним зобов'язанням [7, 8]. Ключовий прийом полягає в перекладі технологічного розвитку на мову марксистської теорії виробничих сил. У марксистській традиції виробничі сили — це головна рушійна сила суспільного прогресу. Відповідно, розвиток штучного інтелекту, квантових обчислень, біотехнологій та воднево-енергетичних систем оголошується «об'єктивно необхідним» — а отже, партійно та юридично обов'язковим. Відставання від цього вектора є відступом від «законів історії» [9]. З правової точки зору це призводить до унікальної конструкції: технологічний пріоритет набуває конституційного статусу. У 2018 році «ідеї Сі Цзіньпіна про соціалізм із китайською специфікою нової ери» були внесені до Конституції КНР (стаття 1), що автоматично надало їм вищої юридичної сили [10]. Будь-яке законодавство у сфері технологій повинне відповідати цим настановам — це і є правова рамка всієї технологічної регуляторики. Варто підкреслити, що подібна конституціоналізація технологічної доктрини є унікальним явищем у порівняльному праві. Конституції більшості держав містять норми щодо захисту прав людини і базових свобод, але не прямих зобов'язань щодо розвитку конкретних технологій. Китайська модель здійснює саме цей крок — перетворюючи партійну програму на конституційний припис [9].

Трифазова модель регулювання. Китай свідомо обрав послідовну, а не превентивну модель регулювання. Перший етап — до 2020 року — характеризувався максимальною дерегуляцією: технологічним компаніям надавалася практично необмежена свобода для зростання, що дозволило Alibaba, Tencent, Bytedance та Baidu увійти до числа найбільших технологічних корпорацій світу. Другий етап — до 2025 року — перехід від програмних документів і гайдлайнів до системного законодавства. Третій етап — до 2030 року — досягнення глобального лідерства з розвиненою регуляторною екосистемою [4, 11]. Ця модель принципово відрізняється від Євросоюзу, де Акт про штучний інтелект (AI Act) формувався майже п'ять років і набув чинності лише у серпні 2024 року [3]. Китай за той самий час уже застосовував діюче законодавство у сфері алгоритмів, дипфейків і генеративного ШІ. Водночас швидкість ухвалення норм поставила під сумнів їх якість: ряд дослідників звертає увагу на внутрішні суперечності між «Тимчасовими положеннями про генеративний ШІ» та «Правилами глибокого синтезу», що свідчить про певний брак міжвідомчої координації [12].

Базовий законодавчий пакет КНР у сфері технологій станом на 2026 рік включає такі ключові акти:

Положення про рекомендаційні алгоритми (березень 2022) — перший у світі акт, що регулює алгоритмічну персоналізацію контенту, встановлює вимоги прозорості та заборону маніпулятивних практик.

Положення про управління технологіями «глибокого синтезу» (січень 2023) — регулювання дипфейків, обов'язкове маркування синтетичного контенту, відповідальність платформ.

Тимчасові положення про генеративний ШІ (серпень 2023) — вимоги безпеки, ліцензування, обов'язковий «політичний фільтр».

Пробні заходи з етичного огляду науково-технічної діяльності (2023) — обов'язкова біоетична і технологічна експертиза досліджень.

Проект Закону про штучний інтелект (2024–2025) — комплексний акт про права на навчальні дані, відповідальність розробників і стандарти безпеки.

Перший національний пакет стандартів для гуманоїдної робототехніки [13] — розроблений за участі понад 120 організацій, охоплює весь життєвий цикл роботів.

Принцип подвійного стандарту. Одна з системних особливостей китайського регулювання — свідоме розмежування між правилами для приватних суб'єктів і для державних органів. Правила розпізнавання облич 2024 року забороняють аналіз расової належності, релігійних переконань і стану здоров'я — але лише для недержавних структур. Для органів безпеки винятки зберігаються [14]. Правова система захищає громадян від корпорацій, але не від держави — це принципова позиція, а не прогалина. Цей принцип є однією з найбільш критикованих особливостей китайської регуляторної моделі в міжнародних правових дискусіях [5].

Обов'язковий політичний фільтр. Найбільш специфічна норма китайського регулювання ШІ — пряме вбудовування цензури в технічну архітектуру. Регуляторні вимоги зобов'язують компанії тестувати ШІ-системи таким чином, щоб вони відхиляли переважну більшість запитів, здатних «підривати державний лад». Це не рекомендація — це ліцензійна умова. Компанія, чия система не відповідає цьому стандарту, не отримає дозволу на діяльність [4]. З порівняльно-правової точки зору, такий механізм є унікальним — ні Акт про ШІ ЄС, ні відповідні регуляторні рамки США не передбачають аналогічного типу попереднього змістовного контролю.

Концепція цивільно-військового злиття є одним із ключових правових механізмів у контексті технологічної стратегії КНР. Вона була зведена в ранг національної стратегії у 2017 році та отримала інституційне підкріплення у вигляді Комісії з розвитку цивільно-військової інтеграції при Центральній військовій раді КНР [5]. Правова суть доктрини полягає в тому, що розмежування між цивільними і військовими науково-дослідними установами фактично ліквідовується. Університети, отримуючи державне фінансування на дослідження у сфері нейроінтерфейсів, квантових обчислень або синтетичної біології, одночасно є суб'єктами нормативних актів Народно-визвольної армії Китаю. Будь-яка розробка потенційно є розробкою подвійного використання — і законодавство не лише допускає, а прямо передбачає цей зв'язок. Наслідком для правового регулювання є те, що «цивільні» закони про технологічну безпеку, захист даних або права інтелектуальної власності не поширюються на оборонні застосування в повному обсязі. Правова система свідомо залишає цей простір у тіні, формуючи правову лакуну на користь держави і армії [15]. Таблиця 1 узагальнює і систематизує питання правових рамок таких технологій [5, 13].

Таблиця 1. Правові рамки технологій подвійного використання у КНР

Технологія	Цивільне застосування	Військове застосування	Правова рамка
Нейроінтерфейси	Реабілітація, медицина	Управління БПЛА, зв'язок	Програма 7 міністерств (2021)
Квантові технології	Криптографія, фінанси	Злам шифрування, ПВО	Стандарти МІІТ
Водень	Транспорт, промисловість	Флот (підводні човни)	План NDRC/NEA 2021–2035
6G	Зв'язок, IoT	Управління роєм БПЛА	Стандарти IMT-2030
Гуманоїдні роботи	Логістика, виробництво	Розмінування, штурм	Держстандарти МІІТ (2026)

СЕКТОРАЛЬНІ НОРМАТИВНІ АКТИ. *Штучний інтелект та гуманоїдна робототехніка.* КНР стала першою країною у світі, яка у 2022–2023 роках ухвалила секторальні нормативні акти з регулювання генеративного ШІ — раніше ЄС, США та Великобританії. Регулювання будується за принципом «безпека через ліцензування»: компанія зобов'язана отримати оцінку безпеки перед публічним запуском системи [4]. Цей підхід принципово відрізняється від ризик-орієнтованої моделі ЄС, де рівень регулювання залежить від класифікації системи за рівнем ризику [3]. У січні 2026 року Міністерство промисловості та інформатизації КНР опублікувало перший у світі національний пакет стандартів для гуманоїдної робототехніки [13]. Стандарти охоплюють вимоги до «мозку та мозочка» втіленого інтелекту, процеси навчання моделей та процедури розгортання. Цей акт закладає фундамент для майбутнього ліцензування бойових роботизованих систем і є прикладом заповнення правового вакууму, що існує на міжнародному рівні у сфері автономних систем.

Правове регулювання *квантових технологій* у КНР відрізняється підкресленою закритістю. На відміну від ШІ чи робототехніки, де існують публічні стандарти і ліцензійні вимоги, квантові дослідження здебільшого регулюються через класифіковані відомчі акти НОАК та секретні стандарти Міністерства державної безпеки [5]. Публічна правова база стандартизує лише цивільне застосування — квантову криптографію та квантовий зв'язок. Показово, що у 2024 році Національний інститут стандартів і технологій США NIST (Національний інститут стандартів і технологій США) затвердив три перших постквантових криптографічних стандарти — FIPS (Федеральні стандарти обробки інформації) 203, 204 і 205 [16]. Це свідчить про те, що загроза «Q-Day» — момент, коли квантовий комп'ютер зможе зламати актуальне шифрування — розглядається провідними державами як реальна і неминуча.

Нейроінтерфейси та біотехнології. Семимністерська програма з розвитку інтерфейсів «мозок-комп'ютер» 2021 року є прикладом жорсткої міжвідомчої координації, де профільне науково-технічне регулювання поєднується з оборонним плануванням [5]. Закон КНР про біобезпеку [17] є одним із найбільш комплексних актів у світі: він регулює патогени, генетичні ресурси, лабораторну безпеку та біологічні агенти. Відповідь США у вигляді Закону BIOSECURE Act, що обмежує співпрацю з низкою китайських біотехнологічних компаній, є правовим виміром технологічної холодної війни.

Правову основу *водневої стратегії* становить «План розвитку водневої промисловості» NDRC (Національна комісія розвитку і реформ Китаю) та NEA (Національна адміністрація з енергетики Китаю) на 2021–2035 роки — документ, що встановлює цільові показники та розподіл компетенцій між центром і регіонами [11]. Конкретні зобов'язання забезпечуються через механізм «зеленого фінансування» — субсидії, зелені облігації та податкові пільги. Об'єкт термоядерного синтезу у М'яньяні функціонує в правовому режимі закритого оборонного підприємства.

КНР активно використовує *міжнародні правові майданчики* для просування власних технологічних стандартів. У сфері телекомунікацій Huawei та ZTE просувають стандарти 5G і 6G через ITU, намагаючись заблокувати або маргіналізувати конкуруючі архітектурні рішення США і ЄС. Держава, що встановлює стандарти 6G, отримує права на стандартно-обов'язкові патенти — і відповідно, роялті та технологічну залежність третіх країн [1]. Навігаційна система «Бейдоу», яка з 2020 року функціонує в повному обсязі, є прикладом успішної реалізації цієї стратегії: вона вже замінила GPS у десятках країн Азії, Африки та Латинської Америки, формуючи технологічну залежність від КНР і, відповідно, правову та геополітичну прив'язку. Ця стратегія є практичним виміром концепції «технологічного суверенітету», яку просуває КПК — і яка, за своєю суттю, є стратегією формування нового міжнародного технологічного порядку під керівництвом Китаю [9].

ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ. Доктрина цивільно-військового злиття означає, що будь-яка технологічна взаємодія з китайськими компаніями — постачання обладнання, спільні до-

слідження, використання платформ — потенційно є взаємодією з оборонно-промисловим комплексом КНР. Це вже не теорія: США, ЄС і Велика Британія ввели нормативні обмеження на використання обладнання Huawei, DJI та низки китайських біотехкомпаній [5]. Для України, що перебуває у стані збройного конфлікту, ризики є прямими та невідкладними.

Квантові технології несуть загрозу «Q-Day» — моменту, коли достатньо потужний квантовий комп'ютер дозволить розшифрувати архіви зашифрованих повідомлень, зібрані сьогодні («harvest now, decrypt later»). Для України, що веде активну військову та дипломатичну діяльність, перехід на квантово-стійке шифрування є не технічним питанням, а правовою та безпековою необхідністю [16]. Аналогічно, стандарти 6G і «Бейдоу» формують технологічну залежність із довгостроковими правовими наслідками.

Послідовність регулювання. Для України, що прагне розвивати технологічний сектор, надмірно деталізоване регулювання на ранньому етапі може стати бар'єром для інвестицій. «Регуляторні пісочниці» — тимчасові зони зниженого регуляторного навантаження для тестування нових технологій — є прийнятним аналогом китайської «дерегуляційної фази» [6].

Стандартизація як стратегія. Україна як кандидат на членство в ЄС має унікальну можливість брати участь у формуванні стандартів ЄС з ШІ, 6G та зеленої енергетики — і тим самим впливати на глобальне технологічне право зсередини найбільшого у світі регуляторного блоку. Це є асиметричним відповідником китайської стратегії просування власних стандартів через ITU (Міжнародний союз електрозв'язку).

Міжвідомча координація. Семимністерська модель координації у сфері нейроінтерфейсів є прикладом ефективного управління міждисциплінарними технологіями. В Україні регулювання нових технологій досі розпорошене між Мінцифри, Мінекономіки, Мінюстом та відомствами безпекового сектора без єдиного координаційного механізму.

На основі проведеного аналізу формулюються такі рекомендації щодо вдосконалення законодавства та регуляторної політики України:

Прийняття Закону України про штучний інтелект на основі AI Act ЄС з адаптацією під безпекові потреби воєнного часу. Ключовий елемент — обов'язкова оцінка технологічного ризику для систем, що використовуються в оборонному секторі.

Законодавче закріплення вимог до квантовостійкого шифрування в державних комунікаціях з урахуванням стандартів NIST FIPS 203, 204, 205 [16].

Нормативне регулювання технологій подвійного використання через розширення законодавства про експортний контроль з урахуванням нейроінтерфейсів, синтетичної біології та квантового обладнання.

Приєднання до міжнародних технологічних коаліцій — ініціатив Quad щодо 6G-стандартів та механізмів ЄС з квантових технологій.

Прийняття Стратегії водневої енергетики України з правовою рамкою, сумісною з European Hydrogen Strategy (REPowerEU).

Формування Міжвідомчого центру технологічної безпеки з координаційними функціями між Мінцифри, Міноборони, СБУ та РНБО.

Запровадження режиму «регуляторних пісочниць» для пілотування нових технологій у визначених секторах з подальшим переходом до повноцінного регулювання.

Висновки. Правове регулювання технологічного розвитку КНР є унікальною конструкцією, де ідеологічне обґрунтування, партійна дисципліна та нормативна техніка утворюють єдине ціле. Марксистська категорія «виробничих сил» слугує конституційно-правовим фундаментом для пріоритизації технологій; доктрина цивільно-військового злиття усуває межу між цивільними та оборонними розробками; а трифазова модель регулювання забезпечує конкурентну перевагу перед більш обережними регуляторними системами Заходу.

Проведений порівняльно-правовий аналіз із застосуванням системного і функціонального методів дозволяє констатувати: китайська модель технологічного регулювання демонструє внутрішню цілісність і стратегічну послі-

довність, що відрізняє її від розрізнених реагувань більшості інших держав на виклики технологічної революції. При цьому ця модель містить структурні риси, несумісні з демократичними правовими системами, — зокрема, принцип подвійного стандарту і обов'язковий політичний фільтр.

Для України ця система становить безпосередні ризики — від квантової загрози зашифрованим комунікаціям до технологічної залежності через стандарти 6G і «Бейдоу». Водночас вона несе конструктивні уроки у сфері швидкого та координованого регулювання нових технологій. В умовах воєнного стану та курсу на євроінтеграцію Україна має унікальну можливість — та нагальну необхідність — сформувати технологічне законодавство, яке поєднує відкритість і безпеку, сумісність зі стандартами ЄС і захист від технологічних загроз з боку авторитарних держав. Зволікання в цій сфері є не нейтральним вибором, а стратегічним програшем у глобальному технологічному суперництві.

Література

1. Dafoe A. AI governance: A research agenda. Future of Humanity Institute, University of Oxford. 2018. URL: https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf

2. Calo R. Artificial intelligence policy: A primer and roadmap. University of California Davis Law Review. 2017. Vol. 51, № 2. P. 399–435. DOI: https://doi.org/10.2139/ssrn.3015350

3. European Parliament. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.

4. Roberts H., Cowls J., Morley J., Taddeo M., Wang V., Floridi L. The Chinese approach to artificial intelligence: An analysis of policy, ethics and regulation. AI & Society. 2021. Vol. 36, № 1. P. 59–77. DOI: https://doi.org/10.1007/s00146-020-00992-2

5. Kania E.B., Costello J. Quantum hegemony? China's ambitions and the challenge to U.S. innovation leadership. Center for a New American Security. 2021. URL: https://www.cnas.org/publications/reports/quantum-hegemony

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2163-19

7. Центральний Комітет КПК. (2025). Пропозиції ЦК КПК до 15-ї п'ятирічної програми соціально-економічного розвитку (5-й пленум ЦК КПК 20-го скликання). Сіньхуа. URL: http://www.xinhuanet.com/

8. Xi J. Develop new quality productive forces [Speech]. Speech at Heilongjiang inspection tour. Xinhua. 2023, September. URL: http://www.xinhuanet.com/

9. Creemers R. China's emerging data protection framework. Journal of Cybersecurity. 2022. Vol. 8, № 1. Article tyac011. DOI: https://doi.org/10.1093/cybsec/tyac011

10. Конституція Китайської Народної Республіки (з поправками 2018 р.). (2018). Всекитайські збори народних представників. URL: https://www.gov.cn/guoqing/2018-03/22/content_5276318.htm

11. National Development and Reform Commission [NDRC] & National Energy Administration [NEA]. (2022). Mid- and long-term plan for the development of the hydrogen energy industry (2021–2035). URL: https://www.ndrc.gov.cn/

12. Webster G., Creemers R., Triolo P., Kania E. (Eds.). China's AI regulations and how they get made. DigiChina, Stanford University. 2022. URL: https://digichina.stanford.edu/work/chinas-ai-regulations-and-how-they-get-made/

13. Ministry of Industry and Information Technology of China [MIIT]. (2026, January). National package of standards for humanoid robotics. MIIT.

14. Cyberspace Administration of China. (2024). Regulations on the management of facial recognition technology. http://www.cac.gov.cn/

15. Cheung T. M. The Chinese defense economy's long march from imitation to innovation. Journal of Strategic Studies. 2016. Vol. 34, № 3. P. 325–354. DOI: https://doi.org/10.1080/01402390.2011.574976

16. National Institute of Standards and Technology [NIST]. (2024). Post-quantum cryptography

standards (FIPS 203, 204, 205). U.S. Department of Commerce. URL: https://www.nist.gov/pqcrypto

17. People's Republic of China. (2021). Biosafety Law of the People's Republic of China. URL: https://www.gov.cn/xinwen/2020-10/17/content_5551667.htm

References

1. Dafoe A. AI governance: A research agenda. Future of Humanity Institute, University of Oxford. 2018. URL: https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf

2. Calo R. Artificial intelligence policy: A primer and roadmap. University of California Davis Law Review. 2017. Vol. 51, № 2. P. 399–435. DOI: https://doi.org/10.2139/ssrn.3015350

3. European Parliament. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.

4. Roberts H., Cowls J., Morley J., Taddeo M., Wang V., Floridi L. The Chinese approach to artificial intelligence: An analysis of policy, ethics and regulation. AI & Society. 2021. Vol. 36, № 1. P. 59–77. DOI: https://doi.org/10.1007/s00146-020-00992-2

5. Kania E.B., Costello J. Quantum hegemony? China's ambitions and the challenge to U.S. innovation leadership. Center for a New American Security. 2021. URL: https://www.cnas.org/publications/reports/quantum-hegemony

6. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny vid 05 zhovt. 2017 r. № 2163-VIII (zi zminamy). URL: https://zakon.rada.gov.ua/laws/show/2163-19

7. Tsentralnyy Komitet KPK. (2025). Propozytsiyi TSK KPK do 15-yi pyatyrichnoyi prohramy sotsialno-ekonomichnoho rozvytku (5-y plenum TSK KPK 20-ho sklykannya). Sinkhua. URL: http://www.xinhuanet.com/

8. Xi J. Develop new quality productive forces [Speech]. Speech at Heilongjiang inspection tour. Xinhua. 2023, September. URL: http://www.xinhuanet.com/

9. Creemers R. China's emerging data protection framework. Journal of Cybersecurity. 2022. Vol. 8, № 1. Article tyac011. DOI: https://doi.org/10.1093/cybsec/tyac011

10. Konstytutsiya Kytays′koyi Narodnoyi Respubliky (z popravkamy 2018 r.). (2018). Vsekytays′ki zbory narodnykh predstavnykiv. URL: https://www.gov.cn/guoqing/2018-03/22/content_5276318.htm

11. National Development and Reform Commission [NDRC] & National Energy Administration [NEA]. (2022). Mid- and long-term plan for the development of the hydrogen energy industry (2021–2035). URL: https://www.ndrc.gov.cn/

12. Webster G., Creemers R., Triolo P., Kania E. (Eds.). China's AI regulations and how they get made. DigiChina, Stanford University. 2022. URL: https://digichina.stanford.edu/work/chinas-ai-regulations-and-how-they-get-made/

13. Ministry of Industry and Information Technology of China [MIIT]. (2026, January). National package of standards for humanoid robotics. MIIT.

14. Cyberspace Administration of China. (2024). Regulations on the management of facial recognition technology. http://www.cac.gov.cn/

15. Cheung T. M. The Chinese defense economy's long march from imitation to innovation. Journal of Strategic Studies. 2016. Vol. 34, № 3. P. 325–354. DOI: https://doi.org/10.1080/01402390.2011.574976

16. National Institute of Standards and Technology [NIST]. (2024). Post-quantum cryptography standards (FIPS 203, 204, 205). U.S. Department of Commerce. URL: https://www.nist.gov/pqcrypto

17. People's Republic of China. (2021). Biosafety Law of the People's Republic of China. URL: https://www.gov.cn/xinwen/2020-10/17/content_5551667.htm

Sofiia Lykhova, Petro Bilenchuk, Tetiana Obikhod

LEGAL REGULATION OF CHINA'S TECHNOLOGICAL DEVELOPMENT AND PROSPECTS FOR UKRAINE

National Aviation University
Liubomyra Huzara Avenue, 1, 03058, Kyiv, Ukraine
European Academy of Human Rights
Legal company «AUR-CONSULTING»
Kharkivske Shosse, 48, 02000, Kyiv, Ukraine
E-mails: k_kpipp@ukr.net, aur.consalt@gmail.com, obikhod@kinr.kiev.ua

The purpose *of the article is to examine the system of legal regulation of technological development of the People's Republic of China in the context of the implementation of the 15th Five-Year Plan (2026–2030) and to develop scientifically grounded recommendations for improving Ukrainian legislation in the field of technological security.* ***Research methods:*** *comparative legal analysis was employed, as well as methods of systemic and functional approaches.* ***Results:*** *the ideological foundation of the concept of "new quality productive forces", which acquired constitutional status, was analyzed; the three-phase model of legal regulation of technologies (deregulation → systemic legislation → global leadership) was investigated; the legal architecture regulating artificial intelligence, quantum technologies, neural interfaces, and hydrogen energy was revealed; the principle of "double standard" for state and private entities was identified; the doctrine of "civil-military fusion" was examined as a key legal mechanism for dual-use technologies; it was established that the PRC surpassed the EU in adopting sectoral acts on AI regulation.* ***Discussion:*** *recommendations for legislative and regulatory policy of Ukraine in the technological sphere under martial law and the European integration course were formulated, in particular: adoption of the Law on Artificial Intelligence based on the EU AI Act; implementation of quantum-resistant encryption according to NIST standards; regulation of dual-use technologies through export control; creation of an Interagency Center for Technological Security; introduction of "regulatory sandboxes"; threats to Ukraine related to the civil-military fusion doctrine, the quantum threat of "Q-Day", and technological dependence through 6G standards and the "Beidou" system were identified.*

Keywords: *technology law; artificial intelligence; civil-military fusion; quantum technologies; China 15th Five-Year Plan; technology security; European integration; Ukraine.*

Дата першого надходження статті до видання: 11.03.2026
Дата прийняття статті до друку після рецензування: 03.04.2026
Дата публікації (оприлюднення) статті: 30.04.2026