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: **«ІНФОРМАЦІЙНА БЕЗПЕКА США В УМОВАХ ГЕОПОЛІТИЧНОЇ КОНКУРЕНЦІЇ З КНР»**

Виконав:
студент 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Бурковський Данило Андрійович
(прізвище, ім'я, по батькові)

Керівник:
к.п.н., доц. Пересипкіна Ірина Валентинівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
к.п.н., доц. Калюжна Юлія Іванівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ – 2025 р.

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

_____ _____ **Наталія ВІННИКОВА**
«_2_» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра
Бурковський Данило Андрійович
(прізвище, ім'я та по батькові)

1. Тема роботи «Інформаційна безпека в умовах геополітичної конкуренції США та КНР»
2. керівник роботи к.п.н., доц. Пересипкіна Ірина Валентинівна
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.
3. Перелік питань, які потрібно розробити:
– Теоретичні підходи до визначення поняття «інформаційна безпека» у системі міжнародних відносин
– Глобальна геополітична конкуренція як новий вимір міжнародного суперництва держав
– Стратегічні підходи до забезпечення інформаційної переваги на міжнародній арені
– Еволюція інформаційної стратегії США: від «інформаційного домінування» до «цифрового стримування»
– Концепція «кіберсуверенітету» та політика «цифрового шовкового шляху» як інформаційні стратегії КНР
– Кіберконфлікти, технологічна конкуренція та боротьба за цифровий суверенітет між США та КНР
– Технологічний, військовий та ідеологічний виміри у стратегічних підходах щодо інформаційної безпеки США та КНР
– Міжнародне співробітництво США у забезпеченні інформаційної безпеки
– Напрямки забезпечення інформаційної безпеки США у протистоянні з КНР: досвід для України

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	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
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: 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти ___ _____Данило БУРКОВСЬКИЙ
(підпис) (ім'я, прізвище)

Керівник роботи _____ _ Ірина ПЕРЕСИПКІНА
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми зумовлена стрімкою трансформацією глобального безпекового середовища, у якому інформаційний простір став ключовим полем стратегічного протистояння. Сучасні процеси цифровізації, зокрема розвиток штучного інтелекту, квантових технологій та глобальних комунікаційних платформ, формують нову архітектуру міжнародної взаємодії, де контроль над інформаційними потоками перетворюється на вирішальний чинник національної могутності. Саме тому, з огляду на посилення КНР, США опиняються перед необхідністю адаптувати свою політику інформаційної безпеки до якісно нових викликів, що охоплюють як кіберсферу, так і інформаційно-психологічний вимір. Варто наголосити, що конкуренція між США та КНР давно вийшла за рамки традиційного військово-політичного суперництва, перетворившись на комплексне змагання за домінування у сфері технологій, стандартів даних та інфраструктури глобального цифрового простору. До того ж, КНР активно розвиває інструменти «цифрового суверенітету» та екосистеми, альтернативні західним, що створює додаткову напругу в питаннях безпеки критичних технологій, інтелектуальної власності та захисту комунікаційних мереж. У цьому контексті інформаційна безпека США набуває подвійного значення: з одного боку, як механізм захисту національної інфраструктури й демократичних інститутів від зовнішнього втручання; з іншого – як інструмент стратегічного стримування та збереження глобального впливу держави.

Ступінь вивченості теми можна охарактеризувати як таку, що динамічно розширюється, проте зберігає певну фрагментарність у змістовому та методологічному вимірах. У вітчизняному науковому дискурсі простежується низка праць, спрямованих на аналіз американської моделі інформаційної безпеки, її інституційної структури та засад державної політики у сфері протидії інформаційним загрозам. Зокрема, вагомий внесок у формування теоретичних засад зробили О. Білоусов [1], О. Пирожик [14], В.

Саранча [17] та С. Стежко [19], які розглядають американський досвід як приклад комплексного та адаптивного підходу до захисту національного інформаційного простору.

Окремий напрям досліджень присвячений безпосередньо загостренню суперництва США та Китаю у сфері інформаційної та кібербезпеки. Тут акцентовано увагу на технологічному змаганні, ескалації кіберзагроз і використанні інструментів інформаційного впливу. У цьому контексті важливими є праці І. Підберезних [15], С. Федонюка [20], а також зарубіжних дослідників С. Алі [24], Дж. Насіба [54], Н. Сінгха [65], Х. Соріано Гатіки [66]. Водночас, як слушно підкреслюють М. Копійка [6] і Д. Вулетич [73], попри значну кількість публікацій, усе ще бракує комплексних міждисциплінарних досліджень, що поєднували б аналіз інформаційної війни, технологічної конкуренції, стратегічних пріоритетів США та специфіку китайської «гострої сили». Недостатньо вивченими залишаються й потенційні наслідки цього протистояння для формування безпекової політики України та її адаптації до нових геоінформаційних реалій.

Мета дослідження – визначити особливості забезпечення інформаційної безпеки США в умовах геополітичної конкуренції з КНР.

Завдання дослідження:

– розглянути теоретичні підходи до визначення поняття «інформаційна безпека» у системі сучасних міжнародних відносин та пов’язану з нею глобальну геополітичну конкуренцію як новий вимір суперництва держав;

– розкрити стратегічні підходи до забезпечення інформаційної переваги на міжнародній арені, зокрема еволюцію інформаційної стратегії США;

– визначити концепцію «кіберсуверенітету» та політику «цифрового шовкового шляху» як ключові інформаційні стратегії КНР у контексті глобального цифрового впливу;

– виявити специфіку кіберконфліктів, технологічної конкуренції та боротьби за цифровий суверенітет між США та КНР, а також технологічний, військовий та ідеологічний виміри їхнього стратегічного протистояння;

– встановити особливості міжнародного співробітництва США у сфері інформаційної безпеки та з'ясувати напрями забезпечення інформаційної стійкості у протистоянні з КНР, визначивши можливі уроки та практичне значення цього досвіду для України.

Об'єкт дослідження – інформаційна безпека держави в умовах геополітичної конкуренції.

Предмет дослідження – механізми забезпечення інформаційної безпеки США в умовах геополітичної конкуренції з КНР.

Теоретико-методологічна база дослідження спирається на комплекс наукових підходів, що дозволяють всебічно інтерпретувати сучасні трансформації міжнародного інформаційного простору та особливості стратегічного протиборства між двома глобальними акторами. Передусім використовується реалістична парадигма, яка дозволяє інтерпретувати розвиток американсько-китайського суперництва як боротьбу за перерозподіл впливу в умовах зростання ролі інформаційних ресурсів. Разом із тим, конструктивістські підходи допомагають пояснити формування стратегічних наративів, зокрема дискурсу про «цифрову автономію» США та «технологічний суверенітет» Китаю, що визначають політику держав у сфері інформаційної безпеки. Методологія кібербезпекових студій забезпечує аналіз інфраструктури критичної інформації, механізмів кіберзагроз і моделей державного регулювання цифрового середовища. У дослідженні застосовуються методи порівняльного аналізу для виявлення відмінностей між американськими та китайськими підходами до контролю даних, штучного інтелекту і кібероборони, а також системний метод, який дає змогу розглядати інформаційну безпеку як багаторівневу структуру, що охоплює державні інститути, приватний сектор і міжнародні союзи. Крім того, використання інституціонального підходу дозволяє проаналізувати нормативно-правові

рамки США та міжнародні режими, у межах яких формуються стандарти поведінки в інформаційному просторі.

Інформаційна база дослідження охоплює широкий комплекс джерел, що дозволяють всебічно відтворити динаміку трансформації американської політики у цифровому та кібернетичному вимірах. Передусім до неї належать офіційні стратегічні документи США, зокрема Національна стратегія кібербезпеки 2023 року, Стратегія національної безпеки 2022 року, а також щорічні звіти Департаменту оборони щодо військових і технологічних спроможностей Китаю. Ці матеріали, будучи результатом урядового аналізу, фіксують ключові загрози для США, зокрема зростання впливу КНР в інформаційній сфері, активізацію китайських кібератак, масштабні програми збору даних та розбудову глобальної цифрової інфраструктури. Крім того, важливою складовою інформаційної бази є аналітичні доповіді провідних американських і міжнародних дослідницьких центрів, таких як RAND Corporation, Center for Strategic and International Studies (CSIS), Brookings Institution. Ці організації пропонують ґрунтовні оцінки наслідків технологічного суперництва між США та КНР, приділяючи значну увагу штучному інтелекту, напівпровідникам, контролю над критичними даними та інформаційним операціям. У цих матеріалах містяться також прогнози щодо ескалації суперництва у сфері дезінформації, що, як відомо, дедалі більше впливає на глобальну безпеку. Водночас значну роль відіграють наукові публікації вітчизняних та зарубіжних дослідників, які забезпечують теоретичне осмислення взаємозв’язку між технологічним розвитком і безпековими пріоритетами.

Практичне значення отриманих результатів. Запропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані органами влади України насамперед у формуванні більш цілісного й стратегічно виваженого підходу до забезпечення національної інформаційної безпеки, що особливо важливо в умовах посилення глобальної конкуренції між США та КНР. Досвід США, які вибудували багаторівневу

систему протидії зовнішнім інформаційним впливам, дозволяє українським державним інституціям краще розуміти логіку сучасних загроз і, відповідно, адаптувати управлінські рішення; у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

Апробація дослідження була здійснена у вигляді публікації тез наукової доповіді для участі у Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, 21 листопада 2025 р.), на тему: «Strategies for ensuring information security of the USA and China in contemporary conditions».

Структура роботи. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 82 найменування. Загальний обсяг роботи становить 89 сторінок, з яких основного тексту – 79 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МІЖНАРОДНИХ ВІДНОСИНАХ

1.1. Теоретичні підходи до визначення поняття «інформаційна безпека» у системі міжнародних відносин

У системі сучасних міжнародних відносин поняття «інформаційна безпека» набуває дедалі більшої складності та багатовимірності, що, своєю чергою, зумовлює появу різних теоретичних підходів до його інтерпретації [11]. Це поняття охоплює не лише технічний або технологічний вимір, а й політичний, правовий, соціокультурний та навіть психологічний аспекти, адже інформація перетворилася на стратегічний ресурс, здатний впливати на політичні процеси, національну стабільність і глобальну рівновагу [5]. Отже, теоретичні підходи до визначення «інформаційної безпеки» у міжнародних відносинах формувалися поступово, у відповідь на трансформації міжнародного середовища, розширення цифрової інфраструктури, а також зростання кількості та складності гібридних загроз.

Передусім варто виокремити реалістичний підхід, відповідно до якого інформаційна безпека розглядається як інструмент забезпечення національної могутності та збереження суверенітету. Згідно з логікою політичного реалізму, держави змагаються між собою за контроль над інформаційними ресурсами, технологіями та каналами комунікації, адже вони визначають здатність впливати на суспільні настрої, перебіг політичних процесів і хід збройних конфліктів. Прикладом може служити послідовна політика США, спрямована на формування «інформаційної переваги» у глобальному масштабі, що проявилася у стратегічних документах Пентагону та у створенні Командування кібернетичних операцій [22]. Так само Китай, спираючись на неореалістичні уявлення про безпеку, сформував концепцію «кіберсуверенітету», яка закріплює повний контроль держави над внутрішнім інформаційним простором та цифровими потоками [6]. У цьому контексті інформаційна безпека набуває характеру «жорсткої сили», а інформаційні

операції, одного з інструментів стримування чи примусу. Поряд із тим, ліберальний підхід пропонує альтернативну інтерпретацію, зосереджену на значенні міжнародних інститутів, норм та режимів у забезпеченні інформаційної безпеки. З огляду на глобальність інформаційного простору, держави неспроможні ефективно протистояти загрозам поодинці, а тому змушені співпрацювати в рамках багатосторонніх структур, зокрема НАТО, ЄС, ОБСЄ або таких спеціалізованих платформ, як Глобальний форум для кіберекспертів чи Будапештська конвенція про кіберзлочинність. У межах ліберальної традиції інформаційна безпека трактується як спільне благо, для збереження якого необхідні узгоджені міжнародні правила, механізми захисту даних, інструменти запобігання втручанню у виборчі процеси, а також прозорість алгоритмів великих платформ [56].

Окреслюючи теоретичні рамки, важливо згадати також конструктивістський підхід, який фокусується на соціальній природі інформаційної безпеки. У межах конструктивізму сутність інформаційної безпеки визначається не лише матеріальними ресурсами чи інфраструктурою, а й смислами, ідентичностями, нормами та дискурсами, які формують уявлення держав про власні інтереси й загрози. Російсько-українська війна супроводжується масштабним інформаційним протистоянням, у межах якого сторони активно конструюють свої наративи для міжнародної аудиторії, а питання інформаційної безпеки набуває характеру боротьби за інтерпретацію реальності [8].

У рамках сучасних досліджень широкого поширення набув також інституціональний підхід, який зосереджується на організаційних механізмах управління інформаційною безпекою. Він виходить із того, що захист інформаційного простору потребує ефективної взаємодії між державними структурами, приватним сектором, науковими установами та громадянським суспільством. У цьому сенсі провідні країни: Сполучені Штати, Велика Британія, Франція, Іспанія, розбудували комплексні інституційні моделі, що

поєднують діяльність національних центрів кібербезпеки, розвідувальних служб, цифрових агентств і спеціалізованих CERT-команд [1, с. 82–89].

Поза тим, окрему увагу привертає мережецентричний підхід, пов’язаний із розвитком теорії мережевих суспільств і визнанням того, що цифровий простір не має чітких кордонів. Сучасні корпорації, як-от Google, Meta, Amazon або SpaceX, володіють ресурсами, які часом перевищують можливості держав у сфері управління цифровими потоками. Показовим є приклад атаки на мережу SolarWinds у 2020 році, коли масштабна кібероперація торкнулася урядових і корпоративних структур одночасно, продемонструвавши вразливість глобальних ланцюгів цифрової взаємодії [21]. Особливої уваги заслуговує технологічний підхід, який аналізує інформаційну безпеку через призму розвитку цифрових технологій. Штучний інтелект, великі дані, квантові обчислення, біометричні системи, усе це розширює можливості як для захисту, так і для інформаційного впливу [12].

Нарешті, значне поширення у XXI столітті здобув гуманітарний підхід, який акцентує на ролі людини у системі інформаційної безпеки. Він виходить із того, що навіть найсучасніші технології не гарантують повного захисту, якщо суспільство не володіє належним рівнем медіаграмотності, стійкості до дезінформації, умінням критично оцінювати дж ерела інформації. Прикладом може бути досвід України після 2014 року, коли саме підвищення спроможності громадян протидіяти пропаганді стало важливим елементом національної політики безпеки [3].

Не менш важливим є також критичний підхід, що сформувався під впливом критичної теорії безпеки та аналізує інформаційну безпеку через призму влади, контролю та суспільних нерівностей. Відповідно до цієї перспективи інформаційна безпека не є нейтральною категорією, а часто використовується державами для виправдання посилення контролю над громадянами, обмеження свободи слова або централізації інформаційних потоків [39]. Прикладом може слугувати практика деяких авторитарних режимів, які під приводом боротьби з кіберзагрозами впроваджують

масштабну систему спостереження, цензури та контролю над цифровими платформами. Критичний підхід дозволяє виявити приховані механізми впливу і підкреслити, що інформаційна безпека може бути використана як інструмент політичної маніпуляції або легітимації недемократичних практик. У зв'язку з цим важливо відзначити зростання ролі концепції «інформаційного суверенітету», яка стала ключовим елементом дискусій про баланс між свободою інформації та захистом державних інтересів. У різних країнах ця концепція має відмінні тлумачення: в Європейському Союзі вона пов'язана передусім із захистом персональних даних і формуванням безпечного цифрового ринку, тоді як у Китаї, з повним контролем держави над інтернетом та обмеженням діяльності іноземних технологічних компаній [6]. США, зі свого боку, акцентують на забезпеченні «відкритого, глобального та інтероперабельного» кіберпростору, що відповідає ліберальній традиції міжнародних відносин, але водночас активно формують інструменти протидії іноземному інформаційному впливу [22]. Таким чином, різні підходи до інформаційного суверенітету підкреслюють, наскільки теоретичні підходи відображають специфіку політичних систем.

Слід також зазначити, що розвиток інформаційної безпеки тісно пов'язаний із еволюцією концепцій національної та глобальної безпеки. Зокрема, після подій 11 вересня 2001 року та стрімкого розширення кіберпростору основні стратегії безпеки провідних держав почали активно інтегрувати положення щодо захисту інформаційної інфраструктури та цифрових комунікацій. Після масштабних кібератак на об'єкти критичної інфраструктури США (наприклад, атаки на Colonial Pipeline у 2021 році) питання інформаційної безпеки стало беззаперечним пріоритетом у національних стратегіях [76]. Європейський Союз своєю чергою ухвалив оновлену Стратегію кібербезпеки (2020 р.), яка зосереджується на зміцненні колективної стійкості та захисті цифрових кордонів ЄС. Проте навіть ці стратегії неможливо адекватно проаналізувати без поєднання щонайменше трьох підходів — реалістичного, інституціонального та технологічного.

Важливо звернути увагу й на те, що питання інформаційної безпеки все більше розглядається крізь призму міждисциплінарності. Так, фахівці з міжнародних відносин співпрацюють із кіберінженерами, психологами, фахівцями з комунікацій, юристами та експертами з медіа. Захист інформаційного простору від дезінформації потребує поєднання технічних інструментів виявлення бот-мереж і тролів, соціологічних досліджень поведінки аудиторій, правових механізмів регулювання медіа та медійної освіти населення [7]. Міждисциплінарні підходи стають не просто бажаними, а необхідними, адже жодна дисципліна не здатна самостійно описати всю складність сучасного інформаційного середовища. Окремої уваги потребує аналіз гібридних загроз, які поєднують інформаційні, кібернетичні, політичні, економічні й навіть військові інструменти впливу. Саме гібридність загроз стала каталізатором оновлення багатьох теоретичних підходів до інформаційної безпеки. Наприклад, вторгнення РФ в Україну у 2022 році супроводжувалося масштабними операціями з дезінформації, кібератаками на урядові установи України, маніпуляціями в соціальних мережах та спробами вплинути на міжнародний порядок денний [8]. У цьому випадку очевидно, що інформаційна безпека не може розглядатися винятково в рамках реалістичного підходу, оскільки стосується не лише держав, а й приватних компаній, соціальних платформ та глобальних аудиторій. Ліберальні та конструктивістські підходи допомагають зрозуміти міжнародну реакцію, тоді як інституціональний, механізми координації дій між державами.

Не можна оминути увагою і правовий підхід, який набуває дедалі більшого значення у зв’язку з необхідністю регулювання діяльності в інтернеті. У межах цього підходу інформаційна безпека визначається як стан захищеності прав і свобод людини, державних інтересів та комунікаційних систем відповідно до міжнародного й національного законодавства. Це охоплює як питання персональних даних (наприклад, GDPR у ЄС), так і протидію кіберзлочинності, захист інтелектуальної власності, регулювання цифрових платформ та штучного інтелекту [18]. Правове розуміння

інформаційної безпеки також має значний вплив на політичні рішення: наприклад, ухвалення ЄС «Акту про штучний інтелект» демонструє зміну підходів до управління ризиками технологій.

Синтезуючи різні концепції, можна стверджувати, що поняття «інформаційна безпека» у міжнародних відносинах є багатовимірним і не зводиться до одного підходу. Воно формується на перетині політичних інтересів держав, глобальних технологічних трендів, нормативних вимог, інституційних практик, соціальних взаємодій і мережевої логіки сучасного світу. Отже, комплексне теоретичне осмислення інформаційної безпеки потребує поєднання різних дослідницьких традицій, кожна з яких уносить власний вклад у пояснення того, як саме інформація, технології та комунікація формують контури безпеки у XXI столітті. У цьому контексті особливо важливо підкреслити, що жоден із теоретичних підходів не може повністю пояснити феномен інформаційної безпеки сам по собі; натомість лише їхня взаємодоповнюваність створює цілісну основу для аналізу. Тому поєднання підходів не лише збагачує теорію, а й має важливі практичні наслідки для державної політики, зокрема у сфері кіберзахисту, національної безпеки та міжнародного співробітництва.

1.2. Глобальна геополітична конкуренція як новий вимір міжнародного суперництва держав

Глобальна геополітична конкуренція дедалі виразніше постає як новий, структурно складніший вимір міжнародного суперництва держав, що формує конфігурацію глобального порядку у XXI столітті. На відміну від попередніх історичних етапів, коли домінували класичні військово-політичні протистояння чи економічні змагання окремих центрів сили, сьогоднішня конкуренція охоплює стратегічні сфери, які визначають не лише безпеку, а й технологічний розвиток, інформаційний вплив, інституційну привабливість та здатність формувати норми міжнародної взаємодії. Причому, як свідчить аналіз подій після 2014 року, а особливо після початку повномасштабного

вторгнення РФ в Україну у 2022 році, саме багатовимірність інструментів суперництва перетворює сучасний міжнародний простір на арену комплексного протиборства, де використовуються вже не тільки класичні засоби державного впливу, а й гібридні, кібернетичні та когнітивні механізми [20]. Насамперед, варто підкреслити, що глобальна конкуренція між провідними державами дедалі більше спирається на контроль за критичними технологіями. Наприклад, суперництво США та Китаю у сфері штучного інтелекту, квантових технологій та напівпровідникових виробництв стало визначальним чинником зовнішньої політики обох держав [52]. Запроваджені Сполученими Штатами у 2022-2023 рр. експортні обмеження щодо високотехнологічного обладнання для китайських компаній, зокрема Semiconductor Manufacturing International Corporation (SMIC), продемонстрували, що технологічний прогрес став невіддільним від логіки національної безпеки [48]. Пекін, зі свого боку, розробив масштабну стратегію «Made in China 2025», у якій задекларовано прагнення досягнути технологічної самодостатності та зменшити залежність від західних виробничих ланцюгів [34]. Усе це створює новий баланс сил, оснований не на кількості ракет чи танків, а на здатності володіти інтелектуальними ресурсами та інноваційними платформами.

У цьому контексті важливою складовою геополітичного суперництва є саме конкуренція моделей розвитку та ціннісних підходів. Дедалі частіше держави змагаються не лише за території чи ресурси, але й за прихильність третіх країн до певної соціально-політичної моделі. США та Європейський Союз, наприклад, просувають принципи демократичного врядування, прав людини та ринкової економіки, тоді як Китай акцентує на моделі «стабільного розвитку», що базується на сильних інституціях держави, керованому ринку та пріоритеті національного суверенітету над транснаціональними зобов’язаннями. Саме тому інвестиційні проєкти КНР, такі як «Один пояс, один шлях» (ініціатива офіційно розпочата у 2013 році), набули не лише економічного, а й політичного характеру, оскільки забезпечують Пекіну вплив

у стратегічно важливих регіонах, від Африки до Центральної Азії, Близького Сходу й Балкан [39]. При цьому, як свідчать події 2020-2025 років, глобальна конкуренція дедалі більше зміщується у цифровий вимір. Кібероперації, кампанії дезінформації, маніпулювання громадською думкою та штучне створення криз довіри стали буденністю міжнародних відносин [21]. Росія, зокрема, активно застосовує інструменти інформаційної війни, від втручання у виборчі процеси в країнах ЄС та США до масштабних кібератак проти України. Наприклад, у січні 2022 року українські державні сайти зазнали масованої кібератаки, коли було зламано системи низки міністерств, а на головних сторінках з'явилися провокативні повідомлення, що мали на меті дестабілізувати суспільну ситуацію. США та Велика Британія у своїх офіційних оцінках прямо пов'язали цю операцію з російськими спецслужбами, підкреслюючи, що кібервтручання є ключовою складовою стратегічного арсеналу РФ [22].

Додатково варто наголосити, що новий вимір глобального суперництва не обмежується цифровою сферою. Значна увага приділяється також контролю за логістичними маршрутами, енергетичними постачаннями та рідкоземельними металами. Після енергетичної кризи 2022 року, спричиненої російськими маніпуляціями з поставками газу до Європи, Європейський Союз змінив стратегічний підхід до енергетичної безпеки та почав активно диверсифікувати постачання, зокрема укладаючи контракти з Катаром, Норвегією та США. У той час Китай, контролюючи близько 70% глобального ринку рідкоземельних металів (дані 2023 року), здобуває додаткові позиції у технологічній конкуренції, оскільки ці матеріали є ключовими для виробництва акумуляторів, електромобілів, сонячних панелей та зброї нового покоління [51]. Усе це супроводжується посиленням боротьби за регіональне лідерство. Туреччина, наприклад, активно просуває свої інтереси у Східному Середземномор'ї, на Південному Кавказі та в Центральній Азії. Події 2020 року, зокрема друга карабаська війна, у якій Туреччина підтримала Азербайджан, продемонстрували здатність Анкари застосовувати комбінацію

військових, дипломатичних та технологічних інструментів для зміцнення власного впливу. Водночас Іран, попри санкційний тиск, активно нарощує ракетні спроможності та поглиблює співпрацю з РФ у сфері безпілотних технологій, що підтверджує, наскільки важливою для держав стала автономність у виробництві високотехнологічних озброєнь.

Одним із найважливіших трендів сучасного суперництва є дедалі відчутніша мілітаризація космічного простору. Запуск Space Force у США у 2019 році, розвиток китайських програм протисупутникової зброї, а також випробування відповідних систем Росією у 2021 році свідчать, що космос перестав бути суто науковим середовищем. Він перетворився на стратегічний фронт, де держави змагаються за домінування у сфері навігаційних систем, телекомунікацій, моніторингу та оборонних технологій [51]. У цьому контексті важливо звернути увагу на роль міжнародних організацій, які все частіше стають майданчиками для змагання стратегічних інтересів. У рамках ООН, наприклад, США та європейські держави просувають концепцію відповідального використання цифрових технологій, тоді як Китай і Росія наполягають на пріоритеті державного суверенітету у кіберпросторі [56].

Разом із тим взаємозалежність держав у глобалізованій економіці не зменшує, а навпаки посилює конкуренцію. США оголосили про виділення понад 50 млрд доларів у рамках CHIPS and Science Act (2022 рік) для розвитку напівпровідникової промисловості [52]. Китай же продовжує масштабні інвестиції у дослідження й розробки, збільшуючи обсяг фінансування R&D до понад 2,5% ВВП у 2023 році. Варто зазначити, що геополітична конкуренція дедалі більше проявляється у боротьбі за інформаційні ресурси та вплив на глобальну думку. Світові медіахолдинги, соціальні мережі, платформи цифрової комунікації перетворилися на стратегічні активи. Боротьба за інтерпретацію подій, наприклад, висвітлення російсько-української війни 2022-2025 рр. стала не менш важливою, ніж бойові дії на полі. Китай, створюючи мережу медіацентрів CGTN та Xinhua по всьому світу, прагне формувати позитивну глобальну картину власної політики [25], тоді як

російські RT та Sputnik спрямовані на підрив довіри до демократичних інституцій та посилення внутрішніх конфліктів у державах Заходу [39]. Так само очевидним стає те, що сучасна геополітична конкуренція виходить за межі класичного міждержавного суперництва і дедалі активніше охоплює сферу глобального врядування, у якій держави змагаються за можливість формувати правила гри [38].

Упродовж 2022-2025 років це проявилося, зокрема, у дискусіях довкола реформування системи міжнародної торгівлі в межах Світової організації торгівлі (СОТ), а також у протистоянні щодо майбутнього реформи Ради Безпеки ООН. США, ЄС, Індія та Японія виступають за розширення представництва глобального Півдня та модернізацію процедур, натомість Китай і Росія прагнуть зберегти статус-кво, розглядаючи інституційні зміни як загрозу власному впливу. Відтак, боротьба за контроль над міжнародними організаціями стає продовженням стратегічного змагання за визначення норм, стандартів і механізмів регулювання. Ключовим елементом цієї боротьби є конкуренція за контроль над інфраструктурою цифрового майбутнього. Суперечки навколо будівництва мереж 5G у ЄС після 2020 року, класичний приклад такого протистояння. Сполучені Штати наполягали на виключенні технологій Huawei через ризики шпигунства, тоді як деякі європейські уряди, хоча й погоджувалися з питаннями безпеки, намагалися зберегти баланс між економічними інтересами та політичним тиском [20]. Урешті-решт більшість країн ЄС ухвалили рішення про обмеження участі Huawei у критичній телекомунікаційній інфраструктурі, що продемонструвало, наскільки тісно у сучасних умовах поєднуються економічні вигоди та питання національної і регіональної безпеки.

Геополітична конкуренція також дедалі активніше проявляється у сфері продовольчої безпеки, що стало особливо помітно після початку російської агресії проти України у 2022 році. Блокування Чорноморських портів, систематичні ракетні удари РФ по українській зерновій інфраструктурі, а також призупинення Росією участі у Чорноморській зерновій ініціативі у липні

2023 року створили глобальні ризики для продовольчих ринків, підвищивши ціни на зерно і поставивши під загрозу продовольчу стабільність держав Африки та Близького Сходу. У відповідь Україна, за підтримки партнерів, зокрема ЄС, розширила альтернативні маршрути експорту через дунайські порти й залізничні коридори. Це стало прикладом того, як локальний конфлікт перетворюється на глобальний чинник геополітичного суперництва у сфері контролю за продовольчими та логістичними мережами. Важливою характеристикою сучасного суперництва є його асиметричність. Нерідко слабші держави створюють значні виклики сильнішим акторам, використовуючи нестандартні засоби впливу. Наприклад, Північна Корея, попри свою економічну слабкість, завдяки активній програмі тестування балістичних ракет (зокрема серії запусків у 2022–2023 роках) продовжує впливати на безпекову архітектуру Східної Азії. Так само Іран через мережу проксі-угруповань у Лівані, Сирії, Ємені та Іраку посилює свій геополітичний вплив, що особливо проявилося після загострення конфлікту на Близькому Сході у жовтні 2023 року [51].

Новим феноменом стає зростання ролі недержавних акторів, які дедалі частіше виступають суб’єктами глобального змагання. Транснаціональні корпорації, такі як Google, Meta, SpaceX чи TikTok, мають вплив, порівнянний або навіть вищий за вплив окремих держав. Наприклад, діяльність Starlink в Україні після 2022 року показала, що інфраструктурні рішення приватної компанії можуть стати критично важливими для обороноздатності держави та її інформаційної стійкості. Водночас TikTok став предметом геополітичних дискусій у США та ЄС, оскільки законодавці наголошували на ризиках витоку даних та інформаційного впливу Китаю. У квітні 2024 року Палата представників США ухвалила закон про примусовий продаж американської частини TikTok або його заборону, що прямо демонструє змішання економічної конкуренції, політики та безпекових вимірів [39]. Цікаво, що у глобальній конкуренції все більше проявляється боротьба за гуманітарні ресурси та інтелектуальний капітал. Держави прагнуть залучати талановитих фахівців,

студентів, науковців і підприємців, адже саме людський потенціал визначає здатність країни технологічно модернізуватися. США, наприклад, у 2023 році активізували програми залучення інженерів і спеціалістів із кібербезпеки, створивши нові візові механізми для STEM-галузей. Китай, зі свого боку, інвестує у глобальні освітні центри та програми академічного обміну, намагаючись створити альтернативні наративи розвитку для країн Азії, Африки й Латинської Америки [46].

Суттєвим чинником геополітичного суперництва стала також екологічна та «зелена» трансформація. Реалізація Європейського зеленого курсу (European Green Deal), ухваленого у 2019 році та активно впроваджуваного у 2020–2024 роках, перетворила ЄС на одного з ключових глобальних акторів у сфері кліматичної політики. Однак боротьба за «зелене» лідерство також породила нові лінії напруженості, наприклад дебати щодо механізму вуглецевого коригування на кордоні (CBAM), який викликав занепокоєння Китаю, Індії та країн Глобального Півдня чере з ймовірне обмеження доступу їхньої продукції на європейський ринок [49]. Особливе місце в системі сучасного суперництва займає Європейський Союз, який активно трансформує свій підхід до глобальної ролі. Після 2022 року ЄС переглянув стратегічні документи, ухваливши у березні 2022 року «Стратегічний компас», комплексний план посилення оборонної та безпекової спроможності Союзу. Це стало відповіддю на агресію РФ проти України та на необхідність формування більш автономної та стійкої Європи. У подальші роки розпочалася активна робота над розвитком оборонної промисловості ЄС, зокрема над програмою EDIRPA (2023 рік), спрямованою на спільні закупівлі озброєнь. Усе це свідчить, що геополітична конкуренція спонукає навіть традиційно «нормативних» акторів посилювати власний силовий та інституційний потенціал.

У найближчі роки, з огляду на тенденції, можна прогнозувати подальше зростання напруженості у сферах штучного інтелекту, оборонних технологій, енергетичної безпеки та інформаційного впливу. Також можна передбачити

поглиблення суперництва за формування норм міжнародної поведінки, особливо в кіберсфері, космосі та цифровій економіці. Водночас дедалі очевиднішим стає факт: у глобальному середовищі, де швидкість змін збільшується, саме адаптивність, інноваційність і стратегічне мислення визначатимуть здатність держав не просто виживати, а й утверджуватися як впливові актори нового світового порядку.

1.3. Стратегічні підходи до забезпечення інформаційної переваги на міжнародній арені

Оскільки у сучасній системі міжнародних відносин інформація перетворилася на ключовий стратегічний ресурс, забезпечення інформаційної переваги стає фундаментальним елементом національної безпеки та зовнішньої політики держав. Саме тому стратегічні підходи до її досягнення формуються на перетині технологічного розвитку, дипломатії, безпекових стратегій, а також глобальної конкуренції за вплив на світовий інформаційний порядок. Важливо підкреслити, що, з огляду на швидкість цифровізації, інформаційна перевага не є статичною категорією, вона потребує постійного оновлення інструментів, адаптації до нових технологій і врахування міжнародних політичних процесів. У цьому контексті держави прагнуть вибудувати багатовимірну систему засобів, що дозволяє не лише захищати власний інформаційний суверенітет, а й активно формувати глобальні інформаційні потоки, стандарти та наративи. Загалом, стратегічні підходи до забезпечення інформаційної переваги охоплюють кілька взаємопов’язаних напрямів: розвиток технологічної інфраструктури, створення ефективних інституцій кібербезпеки, формування наступальної та оборонної інформаційної політики, міжнародне співробітництво, а також інструменти публічної дипломатії та стратегічних комунікацій. Водночас кожна держава робить акцент на тих елементах, які відповідають її політичним пріоритетам, економічним можливостям та геополітичному становищу. Наприклад, Сполучені Штати з початку 2010-х років послідовно інвестують у розвиток

штучного інтелекту для національної оборони [71], тоді як Китай у рамках стратегії «Цифрового шовкового шляху» прагне встановити глобальне лідерство у сфері телекомунікацій і цифрової інфраструктури [34]. Ці два підходи відображають різні моделі формування інформаційної переваги, хоча обидві демонструють стратегічну спрямованість на довгострокове домінування у глобальному інформаційному просторі.

Одним із центральних інструментів забезпечення інформаційної переваги є технологічне лідерство, адже саме воно визначає здатність держави контролювати канали передачі та обробки даних. Розвиток технологій штучного інтелекту, суперкомп'ютерних обчислень, квантових технологій, систем 5G і 6G створює нові можливості й водночас загрози. Як свідчить приклад США, прийняття у 2023 році Національної стратегії кібербезпеки передбачає масштабну модернізацію критичної інформаційної інфраструктури, інвестиції в цифрову оборону, а також партнерство з приватним сектором, який володіє більшістю інноваційних напрацювань [56]. Зокрема, у документі підкреслюється необхідність зміщення акценту з реактивного захисту на проактивне попередження загроз, що відповідає логіці досягнення інформаційної переваги [22].

Не менш показовою є стратегія Китаю, де інформаційна перевага розглядається як елемент довгострокового глобального впливу. Після презентації у 2015 році концепції «Мейд ін Чайна 2025» та подальшої активізації «Цифрового шовкового шляху» Пекін значно розширив присутність власних технологічних компаній у країнах Азії, Африки та Європи [20]. Наприклад, Huawei, попри критику з боку Заходу, продовжує розбудовувати інфраструктуру зв'язку у понад 170 державах, формуючи залежність від китайських технологічних рішень. Такий підхід демонструє, що інформаційна перевага досягається не лише шляхом внутрішнього розвитку, а й експортом технологій, стандартів та інституційних моделей цифрової взаємодії. Важливим виміром стратегічного забезпечення інформаційної переваги є управління даними і цифровий суверенітет. Держави дедалі частіше

наголошують, що контроль над даними, це контроль над економікою, політикою та суспільними процесами. Європейський Союз, наприклад, з 2020 року запроваджує масштабний нормативний пакет Digital Europe та DSA/DMA, який спрямований на формування «європейського цифрового суверенітету». Йдеться не тільки про захист користувачів та регулювання платформ, а й про створення власних екосистем хмарних технологій (GAIA-X), що повинні зменшити залежність від американських та китайських IT-гігантів. Водночас інформаційна перевага неможлива без ефективної структури стратегічних комунікацій, яка дозволяє державі формувати суспільні настрої, просувати власні наративи та нейтралізувати дезінформаційні впливи противників. Показовими є дії України після 2022 року, коли стратегічні комунікації стали одним з елементів національної стійкості [16]. Використання цифрових платформ для інформування світової спільноти, формування прозорих і водночас емоційно насичених меседжів, активна дипломатія у соціальних мережах, усе це забезпечило Україні потужну інформаційну підтримку з боку демократичних держав. Ще одним характерним прикладом є діяльність Центру глобальної взаємодії Державного департаменту США, який відстежує іноземну дезінформацію та протидіє їй у партнерстві з союзниками [39].

Особливе значення у стратегічних підходах до забезпечення інформаційної переваги відіграють кібероперації як інструмент наступальної інформаційної політики. Відповідно до звітів НАТО після 2021 року, кібератаки стають ключовим елементом гібридного впливу, а держави-суперники активно використовують можливості кіберпростору для паралізації критичної інфраструктури, шпигунства та маніпулювання інформаційними потоками. США, Велика Британія та Естонія активно розвивають модель «active cyber defense», яка передбачає попереджувальні дії проти загроз, а не лише реагування на них [22]. До речі, у 2020 році Великобританія створила Національні кіберсили (National Cyber Force), що підкреслює перехід до нового рівня організації інформаційної боротьби, де кібероперації

інтегруються зі стратегічними комунікаціями та розвідкою. Однак стратегічні підходи не зводяться лише до технологій або безпекових структур. Надзвичайно важливою стає інформаційно-психологічна складова, тобто здатність держави впливати на свідомість суспільства та міжнародної аудиторії. Росія, наприклад, послідовно використовує інструменти інформаційно-психологічного впливу для підриву єдності ЄС та НАТО, що було особливо помітно під час виборів у США у 2016 році, кампаній Brexit, а також численних інформаційних операцій, спрямованих на дискредитацію України [73].

Ще одним важливим елементом забезпечення інформаційної переваги є міжнародне співробітництво. З огляду на глобальний характер інформаційних загроз, жодна держава не може протистояти їм самостійно. НАТО, ЄС, «П'ять очей», а також двосторонні кіберпартнерства формують інституційну основу колективної кібербезпеки. Наприклад, у 2022 році ЄС заснував Європейський центр компетенцій у сфері кібербезпеки у Бухаресті, який координує наукові дослідження та обмін технологіями між країнами-членами. У 2023 році у рамках саміту НАТО у Вільнюсі було ухвалено рішення про створення інноваційного фонду для розвитку критичних цифрових технологій, що також спрямовано на зміцнення інформаційної переваги блоку перед агресивними державами. Ще одним важливим напрямом є розвиток людського капіталу та підготовка фахівців з інформаційної безпеки. Сучасні інформаційні операції настільки складні, що потребують не лише технічних компетенцій, а й глибокого розуміння міжнародних відносин, психології, комунікаційних технологій та поведінкової аналітики [10]. Саме тому багато держав інвестують у навчальні програми, створюють кіберполігони та науково-дослідні центри, щоб забезпечити підготовку спеціалістів нового покоління. Показовим є досвід Естонії, де після кібернападів 2007 року був створений Центр кібероборони НАТО у Таллінні. Цей центр став міжнародним майданчиком для обміну досвідом, тренувань та розробки доктрин, що визначають правила поведінки у кіберпросторі [12]. Естонський кейс

демонструє, що інформаційна перевага може бути досягнута навіть невеликою державою, якщо вона інвестує у знання, технології та інституційну координацію.

Водночас ефективність забезпечення інформаційної переваги неможлива без розвитку культури інформаційної стійкості суспільства. Громадяни повинні бути здатними критично сприймати інформацію, розпізнавати маніпуляції та не піддаватися інформаційним впливам, спрямованим на поляризацію соціуму. У цьому контексті ключову роль відіграють освітні програми, громадянське суспільство й медіаорганізації. Так, Фінляндія після 2014 року впровадила системну програму медіаграмотності, що охоплює школи, університети та державні установи. Як результат, країна посідає високі позиції у рейтингах стійкості до дезінформації [69]. Це підтверджує, що інформаційна перевага – це не лише технології та кіберсили, а й здатність суспільства не стати об’єктом зовнішніх маніпуляцій.

Не менш значущим є і правове регулювання інформаційного простору, яке визначає межі використання інформаційних технологій, правила роботи платформ та відповідальність за поширення неправдивих наративів. Прийняття Європейським Союзом Закону про цифрові послуги (DSA) та Закону про цифрові ринки (DMA) у 2022 році стало одним з наймасштабніших кроків з регулювання глобальних платформ [18]. Ці акти зобов’язали технологічні компанії забезпечувати прозорість алгоритмів, швидко реагувати на дезінформацію та усувати вразливості, що можуть становити загрозу для національної безпеки. Отже, держави, які формують нормативні стандарти у глобальному масштабі, не лише захищають власний інформаційний суверенітет, а й забезпечують довгострокову інформаційну перевагу у формуванні світового правопорядку. Важливо додати, що інформаційна перевага у XXI столітті пов’язана також із боротьбою за стандарти майбутніх технологій, таких як квантовий інтернет, автономні системи, штучний інтелект нового покоління. Держави, які першими встановлюють технічні протоколи та стандарти, отримують можливість формувати правила глобальної цифрової

взаємодії. Приклад Китаю, що активно просуває власні стандарти 5G та штучного інтелекту у рамках ООН та Міжнародного союзу електрозв'язку, свідчить про розуміння стратегічної ролі технократичного впливу [34]. У свою чергу, США у 2023-2024 рр. ініціювали створення коаліції з розробки безпечних стандартів штучного інтелекту за участю ЄС, Японії, Південної Кореї та Канади, що продемонструвало формування нових альянсів навколо цифрових технологій [46].

Кульмінацією стратегічних дискусій про інформаційну перевагу стає питання про етичний вимір інформаційної політики. Регулювання штучного інтелекту, захист персональних даних, алгоритмічна прозорість, відповідальність за цифрові операції, усе це створює нові виклики для держав і міжнародних організацій. Дедалі очевиднішим стає те, що інформаційна перевага має балансувати між безпековими інтересами держави та збереженням демократичних цінностей. Зокрема, ЄС у 2024 році ухвалив перший у світі комплексний Акт про штучний інтелект, який встановляє класи ризиків та обмеження на використання небезпечних технологій [43]. Це демонструє прагнення європейських держав забезпечити контроль над технологічними системами та одночасно не допустити перетворення інформаційної політики на інструмент надмірного державного контролю. Важливо наголосити, що інституційна архітектура забезпечення інформаційної переваги постійно ускладнюється, адже держави прагнуть інтегрувати діяльність різних відомств — розвідувальних структур, кіберкомандувань, центрів стратегічних комунікацій, аналітичних агенцій, дипломатичних служб. Така інтеграція дозволяє виробляти єдину стратегію реагування на інформаційні загрози й одночасно координувати наступальні та оборонні інформаційні інструменти [22]. Наприклад, у 2021 році США створили Об'єднаний центр штучного інтелекту у Пентагоні, який має забезпечити синергію між військовими операціями та новітніми цифровими технологіями [1]. Це демонструє, що інформаційна перевага дедалі більше залежить від здатності держав швидко аналізувати дані, застосовувати

передбачувальне моделювання та інтегрувати розвідувальну інформацію у процес ухвалення рішень.

Зазначимо, що стратегічні підходи до забезпечення інформаційної переваги формуються на основі поєднання технологічного розвитку, дипломатичних інструментів, інституційної стійкості та міжнародного співробітництва. Водночас сучасні події, від російсько-української війни до американсько-китайської технологічної конкуренції, демонструють, що інформаційна перевага стає не просто складовою національної безпеки, а ключовим параметром глобального силового балансу. Держави, які здатні ефективно поєднувати технології, стратегії та комунікації, отримують значну перевагу у формуванні міжнародного порядку, у просуванні власних наративів, а також у забезпеченні національної стійкості перед новими викликами епохи цифрової турбулентності.

Висновки до розділу 1

Слід підкреслити, що теоретичні підходи до розуміння поняття «інформаційна безпека» у системі міжнародних відносин формують методологічну основу для оцінки сучасних викликів глобального інформаційного середовища. Інформаційна безпека, як було показано, охоплює не лише технічний і кібернетичний виміри, але й політичний, соціокультурний та комунікативний аспекти, що, у свою чергу, зумовлює її міждисциплінарний характер. Більше того, у сучасних умовах вона постає як структуроутворюючий елемент зовнішньої політики держав, оскільки інформаційний простір дедалі частіше використовується як інструмент впливу, тиску та досягнення стратегічних переваг.

Водночас глобальна геополітична конкуренція стає новим виміром міжнародного суперництва, де інформаційні ресурси перетворюються на ключовий фактор сили. З огляду на це, держави прагнуть не лише зміцнити власні інфраструктури інформаційної безпеки, а й сформувати стійкі механізми протидії зовнішнім інформаційним загрозам, що постійно

еволюціонують. Причому, слід наголосити, що конкуренція відбувається не лише у сфері технологій чи кіберпростору, але й на рівні ідей, цінностей та наративів, які здатні змінювати сприйняття міжнародної реальності та впливати на поведінку як держав, так і суспільств. Саме тому геополітичний вимір інформаційного протиборства фактично визначає нову архітектуру глобальної безпеки.

Відтак стратегічні підходи до забезпечення інформаційної переваги на міжнародній арені передбачають комплекс заходів, що охоплюють розвиток технологічних спроможностей, удосконалення державної політики, формування стратегічних комунікацій та посилення міжнародної координації. Крім того, важливо враховувати, що інформаційна перевага стає можливою лише за умов поєднання оборонних та наступальних інструментів впливу, а також здатності держави адаптуватися до швидких трансформацій глобального середовища. У цьому контексті отримані результати підкреслюють необхідність подальшої інтеграції інформаційної політики у сферу національної безпеки, що забезпечить підвищення стійкості держави та її конкурентоспроможності у світі, де інформація дедалі частіше визначає розподіл сил.

РОЗДІЛ 2. СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США ТА КНР У СУЧАСНИХ УМОВАХ

2.1. Еволюція інформаційної стратегії США: від «інформаційного домінування» до «цифрового стримування»

Еволюція інформаційної стратегії США, яка охоплює період від концепції «інформаційного домінування» 1990-х років до сучасної парадигми «цифрового стримування», відображає глибинні трансформації міжнародного безпекового середовища, технологічного розвитку та зростаючої конкуренції з боку КНР, Росії та інших держав, що прагнуть посилити власний вплив у кібер- та інформаційному просторі [1, с. 84]. Упродовж трьох десятиліть США послідовно адаптували свої підходи до забезпечення інформаційної переваги, що, з одного боку, дозволило Вашингтону зберігати лідерські позиції, а з іншого, вимагало докорінного перегляду стратегічних орієнтирів у відповідь на нові загрози й виклики. Зрештою, сформувалася модель, яку умовно називають «цифровим стримуванням», сутність якої полягає у створенні таких умов, за яких потенційний противник утримуватиметься від агресивних дій у кіберпросторі через ризик непропорційної відповіді або значних політичних, економічних і технологічних втрат [56]. Початок еволюції інформаційної стратегії США слід пов’язувати з кінцем «холодної війни» та стрімким розвитком цифрових технологій. Після операції «Буря в пустелі» (1991), яка чітко продемонструвала ефективність високотехнологічних засобів управління та комунікації, Пентагон і Рада національної безпеки США активно просувають концепцію «інформаційного домінування». Її ключова ідея полягала у здатності контролювати весь спектр інформаційних потоків на театрі бойових дій, забезпечувати власним силам «інформаційну перевагу» та позбавляти її противника [35]. Відповідно до цього бачення, інформація розглядалася як стратегічний ресурс, що визначає результативність військових операцій, а інформаційні технології, як критична інфраструктура, від якої залежить успіх США на глобальному рівні. Показовим у цьому контексті стало

створення у 1990-х роках спеціальних підрозділів інформаційних операцій та перші аналітичні розробки щодо кіберпростору як нового театру воєнних дій.

У 2000-х роках відбувається подальше розширення концептуальної основи американської політики у сфері інформаційної безпеки. Терористичні атаки 11 вересня 2001 року стали радикальним переломним моментом, адже засвідчили вразливість навіть найбільш технологічно розвиненої держави до асиметричних загроз [19]. У відповідь США розпочали масштабну трансформацію своїх безпекових структур, що включала створення Міністерства внутрішньої безпеки (2003), ухвалення доктрини кіберзахисту, посилення контролю над критичною інфраструктурою та розширення можливостей розвідки. У цей період інформаційна стратегія США ще спирається на ідею домінування, але водночас уряд починає усвідомлювати, що абсолютний контроль у цифровій сфері став практично недосяжним через глобалізацію мережі, розвиток соціальних медіа та появу нових акторів, зокрема недержавних. Особливо показовими стали події 2007-2008 років, коли США вперше зіткнулися з масштабними кібератаками проти союзників: Естонії (2007) та Грузії (2008). Ці атаки продемонстрували, що інформаційна сфера перетворилася на повноцінний інструмент геополітичного тиску, а традиційні механізми стримування у військовій сфері виявилися недостатніми [20].

Новий етап розвитку інформаційної стратегії США розпочався після викриттів Е. Сноудена у 2013 році. Розголошення масштабних програм електронного стеження не лише підірвало глобальний авторитет США у сфері цифрової політики, а й спричинило хвилю дискусій щодо меж державного контролю та приватності [1, с. 86]. У відповідь уряд США був змушений реформувати систему нагляду, запровадити нові процедури контролю за діяльністю спецслужб і переглянути принципи міжнародної співпраці у сфері кібербезпеки. Однак найбільш інтенсивний перегляд стратегічних підходів розпочався після 2016 року, коли американські вибори стали об’єктом масштабних інформаційно-психологічних операцій з боку Росії. Уряд США,

реагуючи на ці виклики, вперше офіційно визнав інформаційний простір ареною стратегічного протиборства. У 2018 році була опублікована Національна кіберстратегія США, яка містила тезу про «готовність США здійснювати наступальні кібероперації» для стримування противників [22]. Саме з цього періоду починає формуватися нова парадигма — «цифрове стримування».

Концепція «цифрового стримування» передбачає комплексний підхід, де поєднуються технологічна стійкість, розвиток наступальних кіберспроможностей, розбудова міжнародних альянсів, захист критичної інфраструктури та формування стійкого до інформаційних маніпуляцій суспільства [56]. На відміну від попередньої стратегії домінування, сучасна модель акцентує увагу на взаємному впливі та ризиках, які стримують противника від використання кіберзасобів атак. Показовим прикладом є стратегія кібербезпеки США 2023 року, яка наголошує на відповідальності великих технологічних компаній за безпечність цифрових продуктів, посиленні державного регулювання та необхідності зміцнення міжнародного співробітництва для колективної протидії кібератакам [56]. Окремо підкреслюється важливість об’єднанн я союзників у форматах НАТО, G7, а також нових цифрових коаліцій для протидії КНР, яка активно нарощує глобальний вплив через ініціативи «Цифрового шовкового шляху» та експорт технологій спостереження [20]. Важливим елементом «цифрового стримування» є також наступальні операції. Наприклад, у 2020 році Пентагон підтвердив, що здійснював операції проти російських хакерських угруповань, аби запобігти втручанню у вибори [22]. Подібні дії свідчать, що США переходять від пасивної оборони до активного впливу, демонструючи готовність реагувати асиметрично.

У ширшому контексті інформаційна стратегія США сьогодні охоплює не лише кіберсферу, але й боротьбу з дезінформацією, захист демократичних інститутів, стійкість медіасистеми, контроль за критично важливими технологіями, включно зі штучним інтелектом [56]. Уряд США ініціював

низку угод з технологічними корпораціями щодо етичного використання ШІ, що також є складовою «цифрового стримування». Паралельно Вашингтон розгортає механізми міжнародного тиску на компанії, які сприяють розвитку цифрових інфраструктур КНР. Прикладом є обмеження на використання обладнання Huawei та ZTE у мережах 5G [52, с. 412–420].

До того ж, перехід США до «цифрового стримування» тісно пов'язаний зі зміною характеру глобальної конкуренції. Якщо у 1990-2000-х роках ключовими загрозами були тероризм та регіональні конфлікти, то після 2010 року домінуючим викликом стала системна конкуренція між великими державами [58]. КНР, використовуючи модель «державного капіталізму», державне фінансування високотехнологічних компаній і масштабні проєкти цифрової інфраструктури в Африці, Латинській Америці та Європі, почала активно змінювати баланс сил у глобальному цифровому середовищі [34]. Це спонукало США до більш жорстких заходів, таких як CHIPS and Science Act (2022), спрямований на обмеження експорту чутливих технологій до Китаю, а також посилення контролю за американськими інвестиціями у китайський технологічний сектор [52]. У такий спосіб США реалізують не лише стримування кіберзагроз, а й стримування технологічного розвитку КНР, що є важливим елементом сучасної геополітичної стратегії [20]. Одночасно з цим, інформаційне стримування США починає охоплювати й гуманітарно-комунікативну сферу. Після пандемії COVID-19 2020 року Вашингтон зіткнувся зі зростанням впливу китайських та російських дезінформаційних кампаній, спрямованих на дискредитацію американської системи охорони здоров'я, управління кризами та політичних інститутів [25]. Як наслідок, уряд США посилив співпрацю зі світовими цифровими платформами, зокрема Meta, Google і X (Twitter), щоб оперативно блокувати ворожі інформаційні операції [59]. У 2021–2023 роках було оприлюднено низку звітів, які показали системну діяльність китайських «бот-мереж» у США, спрямовану на поширення поляризаційних наративів. У відповідь Вашингтон посилив дипломатичний тиск на Пекін і розширив можливості розвідки для

відстеження й атрибуції інформаційних атак. Усе це свідчить, що «цифрове стримування» включає також інформаційно-психологічну складову, спрямовану на зменшення ефективності ворожих кампаній [39].

Ще одним важливим кроком у розвитку американської інформаційної стратегії стали ініціативи зі створення міжнародних цифрових альянсів. Зокрема, у 2022 році США запустили «Ініціативу щодо демократій у цифрову епоху» у межах Саміту за демократію, яка передбачає узгодження правил використання технологій, обмін інформацією про кіберзагрози та спільну протидію авторитарним цифровим практикам [56]. Варто згадати також про посилення співпраці у межах НАТО. У 2021 році Альянс ухвалив оновлену політику кібероборони, яка передбачає можливість застосування 5 статті Вашингтонського договору у відповідь на масштабну кібератаку [22]. Хоча це рішення було здебільшого політичним, воно істотно підвищило рівень стримування, адже сигналізувало противникам про можливість колективної відповіді.

До елементів «цифрового стримування» США також належить розвиток засобів штучного інтелекту для кіберзахисту та інформаційної аналітики. У 2023 році Пентагон оголосив про створення програми Replicator, спрямованої на швидке розгортання автономних систем у великій кількості для протидії технологічним перевагам КНР, зокрема у сфері дронів і робототехніки [51]. У сфері інформаційних операцій США активно використовують ШІ для виявлення підроблених відео, бот-мереж і координації інформаційних атак. Подібні заходи не лише посилюють оборону, а й створюють додаткові ризики для противника, який має враховувати можливість ранньої атрибуції та викриття [36]. Важливо й те, що еволюція американської інформаційної стратегії супроводжувалася зміною доктринальних підходів до поняття «силового реагування». Якщо раніше інформаційна сфера розглядалася як допоміжний елемент, то сьогодні вона стала самостійним доменом, де США можуть застосовувати як військові, так і невійськові інструменти [73]. У Національній стратегії оборони США 2022 року підкреслюється, що

кіберпростір є одним з ключових полів конкуренції з Китаєм, а ворожі дії у ньому можуть розглядатися як загроза національній безпеці, що потребує відповідної реакції [26]. Саме тому США створюють багаторівневу систему реагування, від дипломатичних протестів до економічних санкцій і навіть кібератаки у відповідь.

У ширшому вимірі «цифрове стримування» торкається також економічної політики. Санкції проти китайських компаній, обмеження експорту напівпровідників, створення коаліцій із країнами, що виробляють критичні матеріали, усе це елементи стратегічного впливу на можливості КНР у сфері цифрових технологій [48]. Як показали події 2023-2024 років, обмеження на доступ до найсучасніших мікрочипів суттєво ускладнило розвиток китайських систем штучного інтелекту, що прямо вплинуло на здатність Пекіна проводити інформаційні операції нової генерації [71]. Таким чином, технологічні санкції стають інструментом стримування не менш ефективним, ніж кібератаки чи інформаційні контрнаративи. Окрему роль відіграє взаємодія США з приватним сектором. Оскільки понад 80% критично важливої цифрової інфраструктури у США перебуває у приватній власності, держава не може забезпечити інформаційну безпеку без партнерства з бізнесом [55]. У 2022–2024 роках були підписані нові угоди між урядом і провідними технологічними корпораціями щодо обміну даними про загрози, спільного проведення тренувань і розробки безпечних стандартів продуктів. Усе це суттєво підсилює модель «цифрового стримування», роблячи її не суто військовою, а цілісною державно-приватною системою [17].

Загалом еволюція інформаційної стратегії США демонструє поступовий відхід від уявлення про можливість абсолютного контролю над інформаційним простором. Натомість сучасна модель базується на взаємодії, багатоджерельності, коаліційності та превентивності. Вона охоплює всі ключові виміри інформаційної безпеки: військовий, технологічний, дипломатичний, економічний та соціально-комунікативний. Саме тому «цифрове стримування» розглядається як найбільш адекватна відповідь на

виклики XXI століття, коли конкуренція між державами відбувається не лише у фізичному, а й у віртуальному просторі. Перехід від «інформаційного домінування» до «цифрового стримування» став результатом усвідомлення нової реальності, де ключовою метою є не стільки досягнення повного контролю, скільки формування таких умов, за яких агресія у цифровому середовищі стає невигідною та надто ризикованою для противника. Ця парадигма відображає сучасні тенденції розвитку міжнародної безпеки та визначає роль США як лідера у формуванні глобальної системи цифрових правил, норм і практик. Вона також закладає підґрунтя для нової моделі міжнародного порядку, у якій інформаційна та кібербезпека є не периферійними, а центральними елементами геополітичної взаємодії.

2.2. Концепція «кіберсуверенітету» та політика «цифрового шовкового шляху» як інформаційні стратегії КНР

Концепція «кіберсуверенітету» та політика «цифрового шовкового шляху» посідають ключове місце в сучасній інформаційній стратегії КНР, оскільки вони визначають не лише внутрішню архітектуру регулювання цифрового простору, а й окреслюють глобальні амбіції Пекіна у сфері міжнародного інформаційного впливу. В умовах дедалі загостренішої конкуренції між провідними державами світу за контроль над критично важливими даними, інфраструктурою зв’язку та технологічними потоками КНР формує власну модель цифрової взаємодії, що принципово відрізняється від ліберальної західної парадигми. З одного боку, вона передбачає суворий контроль держави над цифровими ресурсами, а з іншого, активну експансію технологічних платформ і телекомунікаційних систем за межі країни. Унаслідок цього Китай прагне не лише зміцнити власну інформаційну безпеку, але й створити альтернативний технологічний порядок, здатний конкурувати з американськими та європейськими моделями управління кіберпростором [20].

Передусім концепція «кіберсуверенітету» (wangluo zhuquan), офіційно представлена китайським керівництвом у 2010-х роках, базується на принципі

абсолютного права держави визначати правила функціонування інформаційного простору в межах національної юрисдикції [61]. Китай наполягає на тому, що інтернет повинен регулюватися так само, як і будь-яка інша сфера державного життя, за допомогою механізмів правового контролю, моніторингу та превентивних заходів. У цьому контексті Пекін просуває ідею, згідно з якою держави мають суверенне право обмежувати доступ до небажаного контенту, контролювати цифрові платформи та здійснювати фільтрацію інформаційних потоків, що надходять із-за кордону. Іншими словами, Китай виступає проти «відкритої мережевої моделі» США, підкреслюючи, що абсолютна свобода інтернету несе ризики для політичної стабільності, культурної ідентичності та економічної безпеки. Симптоматично, що ухвалення у 2017 році Закону про кібербезпеку КНР стало важливим кроком у нормативному закріпленні кіберсуверенітету, адже документ встановив вимоги щодо локалізації даних, посилив контроль за критичною інфраструктурою та зобов’язав приватні компанії співпрацювати з державними органами в питаннях інформаційної безпеки [51].

Більше того, китайська модель кіберсуверенітету передбачає багаторівневу систему моніторингу, включно з алгоритмічним аналізом поведінкових моделей користувачів, що дозволяє державі запобігати поширенню матеріалів, які можуть «загрожувати національній єдності». Наприклад, система «Золотий щит», більш відома на Заході як «Великий китайський файрвол», уже понад два десятиліття слугує інструментом тотального контролю за інформаційним трафіком, блокуючи доступ до таких ресурсів, як Google, Facebook або X(Twitter) [39]. Така практика, безперечно, викликає критику у ліберальних демократіях, проте з точки зору стратегічної логіки Пекіна вона є цілком виправданою. Китайські лідери переконані, що контроль над інформаційним середовищем дозволяє мінімізувати ризики зовнішньої дестабілізації, особливо у контексті зростання напруженості у відносинах зі США, Таїванем або Японією. Тому концепція кіберсуверенітету є своєрідним ідеологічним каркасом, який тримає всю китайську

інфраструктуру інформаційної безпеки. Однак КНР не обмежується внутрішнім укріпленням цифрового простору. Паралельно з цим Китай активно формує глобальний трек свого інформаційного впливу, політику «цифрового шовкового шляху» (Digital Silk Road, DSR), що стала частиною загального проєкту «Один пояс – один шлях» [71]. Ця ініціатива, започаткована у 2015 році, передбачає розбудову міжнародної цифрової інфраструктури шляхом інвестування у телекомунікаційні мережі, дата-центри, системи супутникової навігації, хмарні сервіси та «розумні» міста у країнах Азії, Африки, Латинської Америки й навіть Європи. Наприклад, компанія Huawei бере активну участь у створенні мереж 4G та 5G у Кенії, Пакистані, Саудівській Аравії, а також у країнах Центральної Азії. В Ефіопії, зокрема, Китай проклав понад 6000 км оптоволоконних кабелів і побудував національний дата-центр, що значно посилило залежність місцевої телекомунікаційної інфраструктури від китайських технологій. Аналогічно, у Сербії Пекін реалізує проєкти з побудови «розумного міста» Белграда, забезпечивши уряд системами відеоспостереження з технологіями розпізнавання обличь [31].Усе це свідчить, що цифровий шовковий шлях виконує не лише економічні, а й геополітичні функції. З одного боку, Китай допомагає країнам, що розвиваються, зменшити цифровий розрив, забезпечити доступ до інноваційних технологій і модернізувати свою інфраструктуру. З іншого, він формує глобальну залежність від китайських технологічних стандартів, що у майбутньому дозволяє Пекіну розширити політичний та інформаційний вплив [46]. Такі країни стають більш чутливими до позиції КНР у міжнародних організаціях, зокрема Міжнародному союзі електрозв’язку, де Китай просуває нові стандарти управління інтернетом, що відповідають його уявленням про кіберсуверенітет. Деякі аналітики зазначають, що Digital Silk Road – це інструмент «інформаційної дипломатії», за допомогою якої Китай прагне змінити баланс сил у глобальному кіберпросторі.

Примітно, що цифровий шовковий шлях передбачає створення альтернативних каналів передачі даних, які не контролюються західними державами. Наприклад, у 2021 році Китай та Пакистан завершили будівництво оптоволоконного кабелю довжиною 820 км, який з'єднує провінцію Сіньцзян з пакистанським портом Гвадар. Такий маршрут потенційно дозволяє КНР зменшити залежність від підводних кабелів, контрольованих США та їхніми союзниками. Також в Індонезії китайські компанії створюють масивні дата-центри, які забезпечують альтернативний хмарний сервіс для регіону Південно-Східної Азії. Це дає Пекіну можливість не лише конкурувати з Amazon чи Microsoft Azure, але й впливати на те, які дані зберігаються за межами китайської юрисдикції [67]. Разом із тим політика цифрового шовкового шляху включає і технологічні проєкти військово-стратегічного характеру. Використання супутникової системи «Бейдоу», яка вже з 2020 року працює глобально, дозволяє Китаю запропонувати альтернативу американській GPS [51]. Цей крок має далекосяжні наслідки, оскільки дані про навігацію, логістику і комунікації стають критичними у процесі ведення сучасних конфліктів. Низка держав, зокрема ОАЕ, Таїланд та Іран, уже інтегрували технологію «Бейдоу» у свої військові системи, що посилює військово-політичний вплив Пекіна.

Не можна оминути й того факту, що китайська модель цифрового розвитку активно використовується як інструмент політичної комунікації та ідеологічного впливу. Через державні медіахолдинги, міжнародні мовники на кшталт CGTN, а також за допомогою соціальних мереж Китай поширює наративи про переваги власного підходу до управління інтернетом [39]. Своєю чергою, для країн із нестабільними політичними системами китайська модель здається привабливою, оскільки вона пропонує механізми контролю над громадською думкою та можливість мінімізувати протестні настрої через цифрові важелі. Водночас політика цифрового шовкового шляху не позбавлена критики. Західні держави неодноразово наголошували, що китайські технологічні компанії, які беруть участь у проектах за кордоном, можуть бути

зобов’язані передавати дані китайським спецслужбам згідно з законом КНР. Наприклад, у 2020 році Великобританія відмовилася від використання обладнання Huawei для розгортання мережі 5G, мотивуючи це ризиками для національної безпеки [20]. Подібні побоювання висловлювали США, Канада, Австралія та Японія. Також критику викликають аспекти «технологічного боргу»: деякі африканські країни, отримавши китайські кредити на розвиток цифрової інфраструктури, в подальшому стикаються з фінансовими труднощами, що збільшує їхню залежність від Пекіна.

Попри це, Китай продовжує розширювати глобальну інфраструктуру, підкреслюючи, що цифровий шовковий шлях сприяє розвитку інклюзивної економіки та цифрової трансформації світу. Зокрема, у 2023 році КНР уклала угоди з Саудівською Аравією, Єгиптом та Аргентиною щодо співпраці у сфері штучного інтелекту, кібербезпеки та телекомунікаційних проєктів [39]. Такі домовленості зміцнюють статус Китаю як глобального постачальника технологій та сприяють формуванню нового світового інформаційного порядку. Загалом концепція кіберсуверенітету та політика цифрового шовкового шляху відображають прагнення КНР створити багаторівневу систему міжнародного впливу, де технології стають не лише економічним інструментом, а й елементом стратегічної потуги [34]. Ці два напрями є важливими не лише для розуміння китайської цифрової політики, але й для аналізу глобального перегрупування сил у сфері інформаційної безпеки, де Китай дедалі активніше претендує на роль одного з ключових акторів. У підсумку можна стверджувати, що інформаційні стратегії КНР формують нову парадигму цифрової геополітики, в межах якої держава не лише захищає власний простір, але й прагне трансформувати самі правила функціонування глобального інформаційного середовища.

Більш того, політика КНР у сфері кіберсуверенітету та цифрового шовкового шляху поступово трансформує міжнародні норми і механізми управління глобальним інтернетом, що вже зараз відчутно змінює баланс сил між провідними державами [46]. Китай активно просуває ідею

багатосторонності, під якою розуміє не участь широкого кола недержавних акторів, як це передбачає західна модель мультистейкхолдеризму, а перш за все домінуючу роль держав у визначенні правил цифрової взаємодії. Таким чином, Пекін намагається створити альтернативну систему цінностей, у якій державний контроль розглядається не як обмеження свободи, а як необхідний елемент національної безпеки та суверенітету. Цей підхід, між іншим, знайшов підтримку у низці авторитарних або напівавторитарних режимів, зокрема в Росії, Ірані, Білорусі та Ефіопії, які також просувають ідею «цифрових кордонів» і прагнуть обмежити транснаціональний вплив західних платформ [39]. У межах міжнародних організацій Китай активно працює над просуванням технічних стандартів, які відображають його бачення кіберпростору. Наприклад, у Міжнародному союзі електрозв'язку представники КНР пропонували концепцію «нового інтернет-протоколу», що передбачає централізоване управління мережевою інфраструктурою та розширені можливості моніторингу трафіку [54]. Хоча ця пропозиція викликала значну критику з боку США та країн ЄС, вона продемонструвала наміри Китаю не просто адаптувати існуючу систему до власних інтересів, а фактично створити паралельну технологічну архітектуру, яка могла б стати домінантною для країн Глобального Півдня. Подібні ініціативи свідчать про стратегічний підхід КНР: контроль над стандартами означає контроль над майбутнім цифрової еволюції, а отже й посилення політичного впливу.

Важливим аспектом цифрового шовкового шляху є його роль у зміцненні економічної взаємозалежності між Китаєм та партнерськими державами. Це особливо помітно на прикладі країн Африки, де китайські інвестиції в телекомунікації стали одним із головних стимулів розвитку цифрової економіки [31]. Наприклад, у Руанді китайські компанії створили сучасну систему електронного урядування, що дозволило значно підвищити ефективність адміністрування та доступ громадян до державних послуг. У Нігерії компанія ZTE бере участь у проєктах з розбудови національної інфраструктури кібербезпеки, включно з центрами реагування на комп'ютерні

інциденти. З одного боку, такі ініціативи сприяють технологічній модернізації регіону, але, з іншого, вони поглиблюють залежність країн Африки від китайського програмного та апаратного забезпечення, що у перспективі може трансформуватися в інструмент геополітичного впливу. Не менш показовим є приклад Латинської Америки, де китайські технологічні гіганти активно конкурують з американськими корпораціями. У Бразилії Huawei стала одним із ключових постачальників обладнання для мереж 5G, що викликало серйозну стурбованість у Вашингтоні [71]. У Венесуелі Китай допоміг створити систему соціального моніторингу на основі біометричних даних, що, за деякими оцінками, було використано урядом для контролю за політичною активністю населення. Ці приклади демонструють, як технологічні інструменти можуть перетворюватися на важіль зовнішньополітичного впливу, що дозволяє Пекіну зміцнювати позиції в регіонах, де традиційно домінували США [39].

У внутрішньополітичному контексті концепція кіберсуверенітету дозволяє КНР підтримувати високий рівень інформаційної безпеки та стабільності, що китайське керівництво вважає одним із ключових чинників свого економічного успіху. Однак її значення виходить далеко за межі національних інтересів: фактично Китай пропонує світу альтернативну модель цифрового управління, яка може стати привабливою для держав, що не поділяють ліберальну ідеологію інформаційної своб оди [46]. Саме тому, наприклад, Саудівська Аравія, ОАЕ чи Єгипет активно співпрацюють із Пекіном у сфері штучного інтелекту, технологій безпеки та урбаністичних цифрових рішень. Разом із тим варто зазначити, що цифровий шовковий шлях не є лише інструментом політичної експансії. Він сприймається багатьма державами як реальний шлях до модернізації, адже Китай пропонує відносно дешеві та швидкі технологічні рішення, які здатні скоротити цифровий розрив [31]. На тлі західних проектів розвитку, що часто супроводжуються високими вимогами до політичних реформ або відкритості ринку, китайська модель здається гнучкішою та менш обтяжливою.

Проте, попри стратегічні успіхи, інформаційні стратегії КНР породжують і суттєві виклики для міжнародної безпеки. Зокрема, активне просування кіберсуверенітету підриває універсальність принципів відкритого інтернету, що ускладнює міжнародну співпрацю в боротьбі з кіберзлочинністю, тероризмом чи незаконним обігом даних. Децентралізація цифрового простору, що виникає внаслідок створення множини «національних інтернетів», може призвести до фрагментації глобального кіберпростору, так званого феномену «splinternet» [54]. Така перспектива створює ризики для економічної взаємодії, наукового прогресу та інновацій. Крім того, цифровий шовковий шлях сприяє посиленню глобальної конкуренції між провідними державами. США розглядають китайську експансію як загрозу своїм стратегічним інтересам, що вже призвело до численних торговельно-технологічних обмежень, зокрема санкцій проти Huawei та ZTE [52]. Європейський Союз також проявляє обережність, розробляючи політику «технологічної безпеки», яка дозволяє обмежувати участь китайських компаній у критичній інфраструктурі [71].

Можна стверджувати, що інформаційні стратегії КНР – це не лише внутрішня політика, а й глобальний проєкт із трансформації міжнародного цифрового порядку. Вони кидають виклик існуючим моделям управління інтернетом, створюють нові механізми впливу та водночас відкривають можливості для партнерства. І хоча оцінки ролі Китаю у цифровій сфері залишаються суперечливими, очевидно, що його вплив лише посилюватиметься, формуючи нові параметри глобальної кіберполітики та визначаючи напрями розвитку міжнародної інформаційної безпеки у XXI столітті.

2.3. Кіберконфлікти, технологічна конкуренція та боротьба за цифровий суверенітет між США та КНР

У сучасному контексті кіберконфлікти, технологічна конкуренція та боротьба за цифровий суверенітет між США та КНР у сучасних міжнародних

відносинах набули характеру структурного протистояння, що визначає нову якість глобальної безпеки та політичної взаємодії держав. Попри формальну багатовимірність цього суперництва, його основою є саме прагнення сторін до встановлення контролю над критичною цифровою інфраструктурою, інформаційними потоками та технологічними стандартами, які визначатимуть архітектуру світового порядку на десятиліття вперед. З одного боку, США позиціонують себе як гарант відкритого, інноваційного та ринково орієнтованого цифрового простору, що, втім, не виключає жорстких механізмів контролю та захисту національних інтересів [56]. З іншого боку, Китай, відстоюючи політику «кіберсуверенітету», намагається вибудувати альтернативну модель цифрового управління, де пріоритетом є внутрішній контроль, технологічне самозабезпечення та глобальна експансія китайських платформ і стандартів [39]. Обидві держави, хоча й різними шляхами, прагнуть до домінування в ключових технологіях, передусім у сфері штучного інтелекту, великих даних, 5G та квантових обчислень.

Водночас кіберконфлікти як один із проявів гібридного протистояння стали для обох держав інструментом впливу, котрий забезпечує приховані операції у політичній, економічній та військовій сферах. Зокрема, атакувальні дії, що пов’язуються зі структурами КНР, наприклад, діяльність угруповань APT10 чи APT41, спрямовані на масштабне викрадення інтелектуальної власності, доступ до чутливих даних урядових відомств і приватних корпорацій, а також на встановлення довготривалих прихованих каналів проникнення у мережі супротивника [21]. США, зі свого боку, активно розвивають концепцію «defend forward», яка передбачає перехоплення та нейтралізацію кібератак ще до їхнього фактичного здійснення, що, між іншим, підтвердилося операціями Кіберкомандування США проти інфраструктури іноземних хакерських угруповань у 2018-2022 рр. [22]. У цьому контексті кіберконфлікти перестали бути побічним явищем технологічного прогресу й перетворилися на системне явище, де обидві держави застосовують як відкриті, так і приховані інструменти боротьби, інколи діючи через проксі-

групи або приватні компанії, що ускладнює атрибуцію та міжнародно-правову реакцію.

Технологічна конкуренція між США та КНР має стратегічний характер і, без перебільшення, визначає траєкторії глобального розвитку. Зокрема, саме суперництво за домінування у створенні й впровадженні мереж 5G стало одним із найбільш показових прикладів цього протистояння. Американські санкції проти Huawei у 2019-2020 рр., спрямовані на обмеження доступу китайської компанії до американських мікрочипів і програмного забезпечення, фактично започаткували глобальну «технологічну декуплінг-політику» [52]. Ця політика передбачає поступове розмежування технологічних екосистем США та КНР. У відповідь Китай активізував програму «Made in China 2025» та ініціативи зі створення незалежних виробничих ланцюгів напівпровідників, що, як свідчить приклад компанії SMIC, хоча й стикаються з обмеженнями, проте поступово просуваються вперед [48]. Таким чином, держави прагнуть не лише до зниження залежності від технологій одна одної, але й до встановлення власних сфер впливу у третіх країнах. У сфері штучного інтелекту конкуренція проявляється ще більш виразно. США, опираючись на інноваційну силу приватного сектору, зокрема компаній Google, OpenAI, Microsoft, Nvidia, контролюють більшість розробок у сфері високопродуктивних графічних процесорів та моделей генеративного ШІ. Китай, у свою чергу, активно впроваджує державну політику підтримки ШІ, що відображається у розвитку компаній Baidu, Tencent, Alibaba Cloud, SenseTime, й зосереджується на масштабному використанні штучного інтелекту в державному управлінні, спостереженні та військово-технічних застосуваннях [43]. Саме тому США у 2022 та 2023 роках прийняли рішення про обмеження експорту високотехнологічних чипів до КНР, що стало ще одним підтвердженням жорсткості технологічної конкуренції.

Паралельно формується боротьба за цифровий суверенітет, яка, по суті, передбачає змагання за право визначати глобальні правила функціонування інтернету та цифрових платформ. США відстоюють модель відкритого

інтернету, яка у теоретичному плані ґрунтується на принципах свободи інформації та конкуренції. Проте, як показують приклади законів Cloud Act або численних антимонопольних розслідувань, Вашингтон прагне зберегти контроль над власними технологічними компаніями та їхньою міжнародною діяльністю [56]. Китай, навпаки, просуває концепцію «кіберсуверенітету», яка була офіційно проголошена у 2016 році під час Всесвітньої конференції з інтернету в Учжені [39]. Ця концепція передбачає право держави забезпечувати повний контроль над цифровим середовищем, включно з можливістю блокування іноземних платформ, регулювання контенту та встановлення національних технічних стандартів шифрування і кіберзахисту.

Китайська стратегія цифрового суверенітету тісно пов’язана з глобальним проєктом «Цифрового шовкового шляху», який включає розбудову телекомунікаційних мереж, дата-центрів, хмарних сервісів та супутникових систем у країнах Азії, Африки та Європи [34]. Показовим прикладом є участь Huawei у створенні мереж 4G і 5G у Кенії, Пакистані та Сербії, що забезпечує КНР не лише економічні вигоди, але й політичний вплив через інтеграцію китайських стандартів у національні інфраструктури цих держав. США, зі свого боку, реалізують альтернативні проєкти, спрямовані на підтримку «надійних мереж» (Clean Network Initiative), а також посилюють співпрацю з союзниками у межах рамкових механізмів, таких як Quad або AUKUS, для розвитку безпечних ланцюгів постачання, технологій ШІ та кіберзахисту [40]. Окрім того, боротьба за цифровий суверенітет проявляється й у протистоянні навколо глобальних платформ. Наприклад, дискусії щодо TikTok у США, які у 2023-2024 роках перетворилися на предмет законодавчих ініціатив щодо можливого примусового продажу або блокування платформи, стали показовими для ширшого конфлікту між державами за контроль над даними громадян [71]. США аргументують такі заходи необхідністю захисту від можливого доступу китайських спецслужб до персональних даних користувачів. Китай відповідає симетрично, обмежуючи роботу іноземних компаній, зокрема американських технологічних сервісів, через регуляцію

ринку кібербезпеки та контроль за транснаціональним обміном даними. Таким чином, боротьба за цифровий суверенітет перетворилася на боротьбу суверенітетів за інформаційний простір один одного.

У військовій сфері кіберпростір став критично важливим доменом для стратегічного планування обох держав. США активно впроваджують концепцію інтегрованих бойових можливостей (Joint All-Domain Command and Control – JADC2), яка передбачає уніфікацію різних військових платформ через єдину цифрову інфраструктуру [22]. Китай водночас реалізує стратегію «інформатизації та інтелектуалізації» Народно-визвольної армії Китаю, що включає створення кіберпідрозділів, розвиток квантових комунікацій і систем радіоелектронної боротьби [51]. Конкретним прикладом кіберконфліктів між державами є інцидент 2021 року, коли США й союзники звинуватили Китай у масштабній атаці на сервери Microsoft Exchange, що охопила сотні тисяч систем у понад 100 країнах. У відповідь Китай заявив про політичну мотивованість звинувачень, але інцидент ще більше загострив питання міжнародних норм поведінки у кіберпросторі [21]. Усе це призводить до того, що протистояння США та КНР виходить за межі традиційної логіки стримування і формує нову конфігурацію глобальної цифрової безпеки [54]. Кожна зі сторін намагається не лише зміцнити власні спроможності, але й створити інституційні механізми впливу на інших акторів. США, наприклад, розвивають партнерства у рамках ЄС-США щодо кібербезпеки, а також проводять тренінги з кіберзахисту для країн Балтії та Індо-Тихоокеанського регіону. Китай, через Шанхайську організацію співробітництва просуває ініціативи щодо колективної цифрової безпеки та спільного протистояння «кібертероризму».

У цьому контексті важливим стає питання вироблення міжнародних правил поведінки у цифровому середовищі, адже, як засвідчують останні події, відсутність спільно визнаних норм лише загострює конфлікт [20]. США просувають ідею формування коаліцій демократичних держав для розробки етичних стандартів використання штучного інтелекту, прозорості алгоритмів і

недопущення зловживань цифровими технологіями. Так, у 2023 році Вашингтон підтримав створення «Декларації щодо майбутнього інтернету», у якій було визначено принципи відкритості, безпеки та захисту прав людини в онлайн-просторі [46]. Китай, натомість, ініціює власні міжнародні формати співпраці, наприклад, у рамках BRICS, де пропонує просувати альтернативну нормативну модель цифрової безпеки, що ґрунтується на невтручанні у внутрішні справи й пріоритетності державного контролю над інформаційним середовищем [34]. Це протистояння нормативних підходів фактично формує дві паралельні моделі цифрового світу, між якими інші держави змушені обирати залежно від власних політичних, економічних і безпекових інтересів.

Боротьба за технологічне лідерство між США та КНР також проявляється у сфері космічних технологій і супутникового зв'язку, які є критичними для функціонування глобальних цифрових систем. США, маючи значні переваги завдяки приватним компаніям на кшталт SpaceX, активно розбудовують інфраструктуру супутникового інтернету Starlink, що вже відіграла важливу роль у забезпеченні стійкості зв'язку в Україні під час російської агресії. Китай, реагуючи на такі тенденції, розпочав створення власного сузір'я супутників «Гоасін» і проєкту «Чжу Жун», які мають забезпечити незалежність КНР від західних систем навігації та інформаційної передачі [51]. У межах «Цифрового шовкового шляху» Пекін також пропонує країнам-партнерам інтегруватися у китайські супутникові мережі, що поступово формує альтернативний цифровий космічний простір і, відповідно, посилює глобальне технологічне суперництво [68].

Не менш важливим є питання кіберекономічної безпеки, адже економічні санкції, експортний контроль і регулювання ланцюгів постачання стали ключовими інструментами стратегічного стримування. США, розуміючи критичність напівпровідникової індустрії, активно співпрацюють з Японією, Південною Кореєю, Нідерландами та Тайванем для обмеження можливостей КНР у доступі до передових технологій виробництва чипів [52]. Наприклад, Нідерланди у 2023 році за наполяганням США запровадили обмеження на

експорт обладнання компанії ASML до Китаю, що значно вплинуло на можливості Пекіна щодо розвитку 7-нм та 5-нм техпроцесів [48]. Китай, своєю чергою, відповів санкціями на експорт рідкоземельних матеріалів та галію, необхідних для виробництва високотехнологічної електроніки. Ці взаємні дії демонструють, що технологічна конкуренція стала інструментом економічної війни нового типу, яка не лише формує нову структуру міжнародної торгівлі, але й безпосередньо впливає на глобальні ланцюги виробництва. Боротьба США та КНР за домінування у цифровому просторі має і глибокий ідеологічний вимір. США послідовно наголошують, що відкритість, прозорість і свобода інформації є необхідними умовами розвитку демократичних інститутів. Китай, навпаки, підкреслює важливість стабільності, контролю та безпеки як пріоритетів функціонування цифрового суспільства [66]. Ці відмінні ідеологічні орієнтири зумовлюють різні підходи до регулювання інтернету, управління даними та інтеграції цифрових технологій у державну політику. Відповідно, боротьба за цифровий суверенітет – це не лише технічне чи економічне питання, а й зіткнення двох моделей політичного розвитку, де одна підкреслює важливість індивідуальних прав, а інша, колективної стабільності й контролю держави.

У цьому середовищі кіберконфлікти стають постійним інструментом взаємного тиску. Атаки на критичну інфраструктуру, злам урядових систем, маніпуляції в соціальних мережах, кампанії дезінформації, усе це вже давно сформувало нову реальність стратегічного протиборства [21]. США звинувачують Китай у масштабних кампаніях кібершпигунства, включно з інцидентом Office of Personnel Management 2015 року, під час якого були викрадені персональні дані понад 20 мільйонів американських державних службовців. Китай у відповідь звинувачує США в розробці наступальних кіберінструментів, наприклад, у використанні шкідливого програмного забезпечення Equation Group, яке, за даними дослідників, було пов’язане з Агентством національної безпеки США. Обидві країни офіційно заперечують причетність до атак, що ускладнює вироблення механізмів міжнародної

відповідальності та регульованості. Ще одним аспектом суперництва є роль приватного сектору та транснаціональних корпорацій у формуванні глобальних технологічних потоків. Американські компанії, такі як Meta, Amazon чи Microsoft, володіють величезними хмарними ресурсами та дата-центрами, що забезпечують домінування США у сфері глобальних цифрових послуг. Китай відповідає просуванням власних платформ: WeChat, Alibaba, TikTok, які стають не лише комерц ійними продуктами, але й інструментами міжнародного впливу [39]. Показово, що у країнах Африки, Південно-Східної Азії та Латинської Америки дедалі більше держав інтегрують китайські цифрові рішення, зокрема системи «розумних міст» (smart city) на основі технологій Huawei та Hikvision, що розширює можливості КНР у сфері глобального контролю даних [31].

Нарешті, як демонструє аналіз стратегій обох держав, боротьба за цифровий суверенітет уже давно вийшла за межі економіки та безпеки і стала основою формування нової геополітичної архітектури [49]. США намагаються створити мережу союзників, які поді LYють принципи відкритого інтернету, у той час як Китай активно розбудовує коаліцію держав, що підтримують концепцію державного контролю над цифровою сферою. Відтак світова система поступово еволюціонує у напрямі багаторівневої цифрової біполярності, де кожна з держав формує власну екосистему норм, стандартів і технологічних рішень. Кіберконфлікти, технологічна конкуренція та боротьба за цифровий суверенітет між США та КНР стали визначальним чинником формування міжнародної цифрової політики та архітектури глобальної безпеки. Це протистояння охоплює всі рівні, від стратегічного до індивідуального, і створює нові параметри геополітичної взаємодії у XXI столітті. З огляду на стрімкий розвиток технологій, ступінь інтенсивності цього суперництва лише зростатиме, а його наслідки впливатимуть на вибір стратегічних шляхів для інших держав, зокрема України, які змушені адаптуватися до нової реальності цифрового поділу світу та вибудовувати власну політику кібербезпеки у відповідь на глобальні тенденції.

Висновки до розділу 2

Зазначимо, що еволюція інформаційних стратегій США та Китаю у XXI столітті формує принципово новий вимір глобальної конкуренції, у центрі якого перебуває боротьба за цифровий суверенітет, контроль над інформаційними потоками та стратегічні переваги у сфері високих технологій. Водночас ця конкуренція не обмежується лише технологічними параметрами, оскільки, по-перше, вона охоплює питання міжнародної безпеки, а по-друге, безпосередньо впливає на формування нового світового порядку. Сполучені Штати, еволюціонуючи від концепції «інформаційного домінування» 1990-х і початку 2000-х років до моделі «цифрового стримування», прагнуть забезпечити здатність стримувати суперників у кіберпросторі шляхом розвитку наступальних і оборонних кіберспроможностей, а також шляхом інституційного зміцнення партнерств, зокрема в межах НАТО та ініціативи Joint Cyber Defense Collaborative. При цьому, як свідчить Національна стратегія кібербезпеки США 2023 року, акцент зміщується на відбудову безпечної цифрової екосистеми, протидію авторитарним технологічним моделям та захист критичної інфраструктури.

КНР, навпаки, вибудовує інформаційну стратегію навколо концепції «кіберсуверенітету», що передбачає повний контроль держави над внутрішнім цифровим середовищем і створення альтернативних глобальних мережевих маршрутів через політику «цифрового шовкового шляху». Ця модель, між іншим, орієнтована на формування технологічної залежності партнерів від китайських платформ та інфраструктури, що особливо помітно у сфері 5G, хмарних технологій та штучного інтелекту.

У контексті загострення кіберконфліктів і геополітичної боротьби за стандарти цифрової трансформації суперництво США та КНР перетворюється на структурний чинник міжнародної безпеки. Зрештою, цифровий суверенітет стає не лише категорією державної політики, але й ключовим ресурсом міжнародної влади, від якого залежить стійкість країн до зовнішніх впливів,

здатність до інновацій та ефективність участі у глобальному управлінні. Отже, сучасна конфігурація інформаційно-технологічного протистояння визначає траєкторії розвитку світового порядку, посилюючи роль кіберпростору як критичного геополітичного простору.

РОЗДІЛ 3. НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США У ГЕОПОЛІТИЧНОМУ ПРОТИСТОЯННІ З КНР

3.1. Технологічний, військовий та ідеологічний виміри у стратегічних підходах щодо інформаційної безпеки США та КНР

Інформаційна безпека в умовах сучасної глобальної конкуренції постає не лише як технічний чи навіть політичний виклик, а як комплексний феномен, у якому технологічні, військові та ідеологічні виміри взаємодоповнюють і взаємопідсилюють один одного. Саме тому стратегічні підходи США та КНР до забезпечення інформаційної безпеки набувають принципово різних конфігурацій, хоча, здавалося б, формально мають спільну мету – захист власного інформаційного простору й здобуття переваги в глобальній кібер- та інформаційній екосистемі. З одного боку, Сполучені Штати зосереджуються на концепції «інформаційної переваги» (information superiority), що передбачає технологічне домінування як основу безпеки. З іншого, Китай вибудовує модель «кіберсуверенітету», поєднуючи контроль над інформаційними потоками з активним просуванням ідеологічних наративів і створенням альтернативних технологічних стандартів [73]. Однак, що особливо показово, обидві держави інтегрують свої стратегічні підходи у ширші контексти національної безпеки, оборонного планування та міжнародної політики, тим самим перетворюючи інформаційну безпеку на один із ключових інструментів геополітичного впливу.

Таблиця 3.1.

Технологічний, військовий та ідеологічний виміри у стратегічних підходах щодо інформаційної безпеки США та КНР

Вимір	США	КНР
Технологічний	Пріоритет на інноваціях: штучний інтелект, квантові технології, мікроелектроніка.	Стратегія «Цифровий шовковий шлях» для розширення глобального технологічного впливу.

	Обмеження доступу КНР до високотехнологічних компонентів (експортні санкції на чипи та обладнання). Розвиток безпечних ланцюгів постачання, ініціативи щодо 5G без Huawei.	Інвестиції в 5G/6G, штучний інтелект та контроль над глобальними даними. Державна підтримка компаній Huawei, ZTE, ByteDance.
Військовий	Кіберкомандування США як окремий вид збройних сил. Активна оборона і проактивні операції в кіберпросторі. Співпраця з NATO у сфері кібероборони, спільні навчання (Cyber Coalition).	Інтеграція кібервійськ до Народно-визвольної армії Китаю. Доктрина «інформаційної перемоги» та злиття військових і цивільних ресурсів. Кібероперації для розвідки, шпигунства та впливу на критичну інфраструктуру інших держав.
Ідеологічний	Наголос на захисті демократії, прозорості, свободі слова та відкритому інтернеті. Протидія дезінформації через Global Engagement Center. Формування глобальних коаліцій на основі демократичних цінностей.	Концепція «кіберсуверенітету» та контроль держави над інформаційним простором. Масштабні внутрішні цензурні механізми (Великий китайський файрвол). Поширення прорежимних наративів через цифрові платформи та медіагрупи.

У технологічному вимірі домінування США історично ґрунтується на інноваційній спроможності приватного сектору та потужній екосистемі університетів, дослідницьких лабораторій і стартапів. Наприклад, мережеві технології, хмарні сервіси, штучний інтелект і супутникові системи зв’язку на кшталт Starlink формують основу американського підходу до побудови

цифрової інфраструктури, здатної витримувати зовнішні атаки та одночасно забезпечувати підтримку глобальних операцій. Ба більше, в Національній стратегії кібербезпеки США 2023 року прямо зазначається необхідність переходу до моделі «колективної кіберстійкості», коли держава, бізнес і громадянське суспільство об'єднують зусилля проти складних загроз [56]. Водночас Китай, як відомо, робить ставку на масштабні державні інвестиції в стратегічні технології, насамперед 5G, квантові обчислення та штучний інтелект. Зазначимо, що в межах ініціативи «Цифровий шовковий шлях» Пекін активно експортує обладнання Huawei, технології відеоспостереження і цифрового контролю, тим самим створюючи інфраструктурну залежність партнерських країн і розширюючи власний геоекономічний вплив [34]. Як наслідок, технологічне змагання між США та КНР дедалі частіше подається не як конкуренція двох ринкових моделей, а як боротьба між відкритою і закритою архітектурами цифрового світу, де питання стандартів, кіберетики та контролю над даними стають визначальними для світової політики.

У військовому вимірі інформаційна безпека США давно інтегрована в оборонну доктрину. Після прийняття Доктрини інформаційних операцій ще у 1990-х роках Сполучені Штати послідовно формували концепцію ведення операцій у кіберпросторі, яка згодом перетворилась на один із ключових напрямів діяльності Кіберкомандування США. Нині американські збройні сили активно впроваджують стратегію «об'єднаних багатодоменних операцій», що передбачає використання інформаційних, кібернетичних, космічних і класичних військових інструментів у єдиному оперативному середовищі [22]. Наприклад, під час операцій проти терористичних угруповань США застосовували комбінацію кібератак, психологічних операцій та перехоплення комунікацій для нейтралізації каналів координації противника. На відміну від цього, китайська Народно-визвольна армія дотримується концепції «Інтегрованого об'єднаного бою», де інформаційний компонент не просто підтримує дії військ, а є фундаментальною передумовою досягнення перемоги. У документах КНР відкрито декларується необхідність

«контролювати інформаційне середовище» й, у разі потреби, «паралізувати системи управління противника на ранньому етапі конфлікту» [51]. Згідно з доповідями Пентагону за 2022-2024 рр., Китай активно розвиває кібернетичні війська, здатні здійснювати кібершпигунство, втручання в критичну інфраструктуру та інформаційні операції в глобальному масштабі. Це включає не лише атаки на урядові системи США, а й кампанії впливу, спрямовані на маніпуляцію громадською думкою в інших державах, зокрема у країнах Південно-Східної Азії та Європи.

Ідеологічний вимір стратегічної конкуренції США та КНР, безперечно, є не менш значущим, ніж технологічний чи військовий. Американський підхід традиційно ґрунтується на просуванні принципів відкритості, свободи слова, вільного ринку і недопущення державного контролю над інформаційним середовищем. Інститути «м'якої сили», зокрема USAID, NED, медіаплатформи Voice of America та Radio Free Europe/Radio Liberty, а також тисячі освітніх програм, спрямованих на підтримку демократичних практик, є ключовими елементами інформаційного впливу США [16]. У контексті глобальної конкуренції з КНР Вашингтон дедалі частіше наголошує на важливості захисту демократичних норм від авторитарних моделей цифрового контролю. У Стратегії національної безпеки США 2022 року прямо стверджується, що Китай прагне «переформатувати міжнародни й порядок на свою користь», використовуючи інформаційні інструменти як засіб політичного тиску [26]. Китайська ідеологічна модель, навпаки, спирається на концепцію «керованого інформаційного простору», де свобода слова підпорядковується завданню суспільної стабільності та збереження політичного контролю. Пекін активно застосовує державне регулювання інтернету, запроваджує обмеження на діяльність технологічних компаній і створює власні інформаційні наративи, спрямовані на зміцнення образу КНР як альтернативного центру глобального розвитку. Ці наративи поширюються через CGTN, Xinhua, China Daily, а також через розгалужену мережу центрів Конфуція, які формують уявлення про Китай як про миролюбну, технологічну та стабільну державу [39]. Водночас

КНР застосовує методи «гострої сили», зокрема інформаційні кампанії, що мають на меті дискредитувати політиків, інституції чи дії інших держав [6]. Відомими є випадки втручання китайських структур у виборчі процеси на Тайвані, спроби впливу на студентські кампуси США або організація інформаційних атак проти ЄС у період пандемії COVID-19. Такі приклади засвідчують, наскільки ідеологічний вимір перетворився на інструмент стратегічного балансування Китаю в глобальному просторі.

Коли технологічні, військові та ідеологічні виміри накладаються один на одного, формується мозаїчна система стратегій, у межах якої США та КНР вибудовують власні конкурентні моделі інформаційної безпеки. У рамках американського підходу пріоритетним стає зміцнення альянсів, від НАТО до Індо-Тихоокеанського партнерства, з метою створення глобальної коаліції протидії авторитарним технологічним платформам [40]. Зокрема, ініціатива «Partnership for Global Infrastructure and Investment», започаткована у 2022 році, передбачає фінансування альтернативних інфраструктурних проєктів у країнах, де спостерігається посилення впливу «Цифрового шовкового шляху». Водночас США нарощують свою присутність у сфері захисту критичної інфраструктури, створюючи міжнародні групи для реагування на кібератаки та обмін найкращими практиками. Пекін, у свою чергу, прагне створити власні мережі партнерств, зокрема в Африці, Латинській Америці та Центральній Азії, де технологічні рішення Huawei, ZTE та інших компаній пропонуються в пакеті з навчальними програмами, фінансовими інвестиціями й політичним супроводом. Такі практики дозволяють КНР формувати залежність держав не лише від технологій, а й від інформаційних стандартів. Наприклад, запровадження китайських систем відеоспостереження у Замбії або Пакистані створює особливий режим інформаційного контролю, що сприяє поширенню китайських моделей управління та наративів [25].

У цій новій архітектурі, що поступово оформлюється, дедалі очевиднішою стає взаємозалежність між внутрішніми політичними процесами держав та їхньою здатністю проектувати інформаційну силу назовні. Зокрема,

США наполягають на збереженні відкритого глобального інтернету та інклюзивної цифрової екосистеми, що передбачає мінімальне втручання держави у функціонування приватного сектору. Така модель, як показує практика, стимулює розвиток інновацій, але водночас залишає простір для зростання зовнішніх загроз — зокрема з боку державних і недержавних акторів, що використовують лазівки в захисті комерційних платформ. Це підтверджують численні кейси кібершпигунства, наприклад атака SolarWinds 2020 року, що зачепила урядові установи США і продемонструвала вразливість навіть найрозвиненіших кіберзахисних систем [21]. США відповідають на такі виклики посиленням партнерства з приватними корпораціями: Microsoft, Google, Amazon Web Services та іншими, які відіграють ключову роль у забезпеченні безпеки національного інформаційного простору [55]. КНР, натомість, прагне зменшити залежність від іноземних технологій та поступово вибудувати автономну екосистему цифрового розвитку [52]. Програма «Made in China 2025», а також інші промислові ініціативи спрямовані на створення власних мікрочипів, операційних систем та захищених телекомунікаційних платформ [42]. Ба більше, Китай розробляє альтернативні протоколи інтернету, зокрема так званий «New IP», що потенційно можуть змінити принципи функціонування глобальної мережі та посилити державний контроль над її інфраструктурою [33]. Це викликає занепокоєння у США та їхніх союзників, оскільки створює ризик фрагментації інтернету на окремі політичні зони з різними стандартами доступу, безпеки й контролю [20]. Уже сьогодні фермери в Ефіопії чи Лаосі, користуючись китайськими технологіями, фактично інтегровані в інформаційний простір, де домінують комунікаційні платформи та наративи КНР, а не Заходу [31].

У військово-політичному аспекті важливою тенденцією стає поступове зближення кібероперацій та інформаційно-психологічного впливу. Саме тут особливо виразно простежуються відмінності між США та КНР. Вашингтон робить наголос на стримуванні противника через демонстрацію спроможності до «активного кіберзахисту», тобто можливості завдавати удару у відповідь,

паралізувати ворожі мережі або здійснювати точкові операції проти інфраструктури противника [22]. Прикладом може слугувати операція американського Кіберкомандування у 2018 році, коли було тимчасово виведено з ладу сервери російської «фабрики тролів» під час проміжних виборів у США. У цьому випадку військовий та інформаційний компоненти були поєднані з метою захисту демократичних процесів [73]. КНР, навпаки, розглядає інформаційні та кібернетичні операції як невід'ємний елемент довготривалої «боротьби без війни», коли основним завданням стає поступове формування сприятливого стратегічного середовища [34]. Це проявляється у використанні прихованих інформаційних впливів, поширенні дезінформації, тиску на іноземні медіа та створенні про-китайських громадських рухів у різних країнах [39]. Такі інформаційні кампанії не супроводжуються прямими кібердарами, але мають не менш довгостроковий вплив, формуючи бажану суспільну думку [59].

Коли ж аналізувати стратегічні підходи обох держав комплексно, стає очевидно, що інформаційна безпека перестає бути суто технічним питанням і перетворюється на основу глобального ідеологічного протистояння. США, з одного боку, апелюють до універсальних цінностей свободи та відкритості, намагаючись сформувати міжнародні коаліції навколо цих принципів [56]. КНР, з іншого, пропонує альтернативну модель, яка акцентує на стабільності, ієрархічності та державному керівництві [61]. Ці дві парадигми дедалі частіше стикаються у міжнародних організаціях, наприклад у рамках ITU чи ООН, де кожна сторона просуває власні стандарти цифрового розвитку [46]. Загалом, технологічний, військовий та ідеологічний виміри інформаційної безпеки США та КНР утворюють складний конфліктний трикутник, у якому кожний елемент підсилює інші [20]. Інновації стимулюють перебудову військових стратегій; військові стратегії, своєю чергою, формують ідеологічні наративи; а ідеологія впливає на те, як суспільства сприймають технології та ставляться до державного контролю. Саме тому глобальне протистояння США й Китаю в інформаційній сфері набуває ознак системного, тривалого та багатоетапного

процесу, який визначатиме характер міжнародних відносин у найближчі десятиліття [51].

І хоча обидві моделі мають свої сильні сторони, їхнє співіснування неминуче призводитиме до подальшої поляризації інформаційного простору. Водночас, як показує аналіз, країни, що перебувають між двома полюсами впливу, вимушені будуть виробляти багатовекторні стратегії інформаційної безпеки, адаптуючи окремі елементи американських та китайських підходів до власних умов. У цьому сенсі глобальна боротьба за інформаційну перевагу стає не лише змаганням двох наддержав, а й поштовхом для формування нових моделей безпеки серед інших держав, передусім тих, що стоять перед викликами гібридної війни. Конкуренція США та КНР у технологічному, військовому та ідеологічному вимірах поступово формує нову архітектуру світового порядку, де інформаційна безпека виступає центральним ресурсом сили. І те, наскільки ефективно держави зможуть інтегрувати ці виміри у власні стратегії, значною мірою визначатиме їхню стійкість, міжнародний авторитет та спроможність протистояти сучасним і майбутнім загрозам.

3.2. Міжнародне співробітництво США у забезпеченні інформаційної безпеки

Міжнародне співробітництво США у сфері забезпечення інформаційної безпеки стало одним із ключових стратегічних напрямів зовнішньої політики Вашингтона, оскільки саме глобальний характер кіберзагроз і швидкість їх транснаціонального поширення вимагають координації зусиль з великою кількістю держав і міжнародних організацій. Відомо, що інформаційні атаки не визнають кордонів, отже, ефективність протидії залежить від здатності держав створювати спільні механізми реагування. Саме тому США упродовж двох останніх десятиліть активно розбудовують мережу двосторонніх і багатосторонніх форматів співробітництва, які охоплюють як технічний, так і політико-стратегічний рівні взаємодії. Хоча масштаби та інтенсивність партнерства варіюються, загальною тенденцією є поглиблення союзницьких

відносин у кіберсфері, що дозволяє Вашингтону формувати глобальну архітектуру інформаційної безпеки, здатну стримувати діяльність недружніх держав і недержавних акторів. Передусім необхідно зазначити, що одним із найважливіших форматів міжнародної взаємодії США є співпраця в межах НАТО. Альянс ще у 2016 році визнав кіберпростір окремою операційною сферою, що стало вирішальним кроком у перетворенні питань інформаційної безпеки на один із пріоритетів колективної оборони [22]. США відіграли ключову роль у розробці підходів до застосування П'ятої статті Північноатлантичного договору у випадку масштабних кібернападів. Наприклад, після інциденту з масованою кібератакою на Естонію у 2007 році саме Вашингтон ініціював створення Центру кібероборони НАТО в Таллінні, який згодом став провідним аналітичним та освітнім майданчиком з кібербезпеки. Важливо й те, що США активно підтримують держави-члени Альянсу в процесі модернізації їхніх кіберспроможностей, передаючи технології, беручи участь у спільних навчаннях («Cyber Coalition», «Locked Shields») і забезпечуючи обмін розвідувальними даними [19].

Поряд із НАТО США поглиблюють співробітництво в рамках «Групи семи» (G7). Тут особливого значення набуває координація політики щодо протидії дезінформаційним кампаніям і втручанню у виборчі процеси. Власне, після президентських виборів у США 2016 року Вашингтон запропонував розширити діяльність спільної Робочої групи G7 з кібербезпеки, яка почала розробляти стандарти швидкого обміну інформацією між державами про виявлені атаки, а також стратегії стримування держав, що здійснюють інформаційні операції [56]. Як приклад можна навести узгоджені заяви G7 у 2021 та 2022 роках, спрямовані проти кіберактивності Китаю та Росії, що демонструє здатність західних країн виступати спільним фронтом проти деструктивних практик конкурентів США.

Не менш важливим напрямом є двосторонні стратегічні партнерства. США, зокрема, мають розвинену систему кібердіалогів із Великою Британією, Канадою, Австралією та Новою Зеландією — державами, що входять до

розвідувального альянсу «Five Eyes». Ця платформа забезпечує глибокий обмін секретною інформацією щодо кібератак, алгоритмів шкідливого програмного забезпечення та нових інструментів боротьби з ними [1]. Власне, саме інтегрованість розвідувальних структур «Five Eyes» дозволила США у 2020–2023 роках оперативно виявляти масштабні атаки з боку китайських хакерських угруповань, таких як «Volt Typhoon» чи «Hafnium» [21]. Крім того, Сполучені Штати посилюють співпрацю з Японією та Південною Кореєю в межах тристороннього формату, який останніми роками дедалі більше фокусується на стримуванні КНР у кібер- та інформаційній сферах [40]. США також посилюють участь у міжнародних організаціях, де формуються стандарти цифрової безпеки. Наприклад, в ООН Вашингтон активно підтримує роботу Групи урядових експертів з відповідальної поведінки держав у кіберпросторі, яка просуває ідеї щодо заборони атак на критичну інфраструктуру і забезпечення прозорості поведінки держав у цифровій сфері [55]. Водночас США критикують ініціативи КНР і Росії щодо розробки альтернативних нормативних підходів, які передбачають жорсткіший державний контроль над інтернетом і суперечать принципам відкритості та свободи інформації. У цьому контексті міжнародне співробітництво стає не лише засобом технічної координації, а й інструментом боротьби за домінування у формуванні міжнародних правил.

Крім того, США створюють та підтримують регіональні ініціативи, спрямовані на допомогу країнам, що розвиваються, у зміцненні їхньої інформаційної стійкості. Наприклад, програма Cybersecurity Capacity Building надає технічну допомогу державам Південно-Східної Азії та Африки у створенні систем раннього виявлення кібератак, розбудові CERT-підрозділів і розробці стратегій кібербезпеки [56]. Такі програми одночасно вирішують два завдання: зміцнюють глобальну цифрову стійкість і розширюють політичний вплив США у регіонах, де активно конкурує Китай. Слід наголосити й на важливості участі США в діяльності Європейського Союзу у сфері безпеки даних та кіберстійкості. Попри те що США не є членом ЄС, співробітництво

між ними, зокрема в рамках угод щодо трансферу даних (EU–US Data Privacy Framewor k, ухвалений у 2023 році), має виняткове значення для формування єдиних стандартів захисту персональних даних та безпечного функціонування цифрових платформ [57]. Після скасування «Щита конфіденційності» Європейським судом у 2020 році США провели масштабну реформу процедур доступу спецслужб до даних іноземних громадян, а також запропонували нові гарантії захисту приватної інформації. Кібердипломатія США виявляється також у розбудові партнерства з технологічним сектором у глобальному вимірі. Оскільки великі корпорації, такі як Microsoft, Google чи Amazon, володіють критично важливими цифровими сервісами, США виступають ініціатором створення «публічно-приватних альянсів безпеки», у межах яких здійснюється обмін технічними індикаторами атак, спільне розслідування інцидентів і розробка стандартів безпеки для хмарної інфраструктури [55]. Як приклад можна навести операцію щодо нейтралізації ботнету Trickbot у 2020 році, яка стала можливою завдяки взаємодії ФБР та провідних компаній.

Помітної динаміки набуває і співробітництво США з Україною, особливо після 2014 року, коли почалася інтенсивна трансформація українського сектору безпеки у відповідь на російську агресію. США не лише надають технічну допомогу українським органам безпеки та кіберпідрозділам, а й сприяють інтеграції України у глобальні мережі обміну інформацією щодо кіберзагроз [14]. Після широкомасштабного вторгнення РФ у 2022 році Вашингтон активізував допомогу, зокрема, передаючи обладнання для захисту критичної інфраструктури, забезпечуючи участь України у спільних кібернавчаннях та сприяючи відновленню цифрових систем після атак на енергетичну інфраструктуру.

Водночас варто врахувати, що співробітництво США у сфері інформаційної безпеки має й важливий елемент стратегічного стримування, який, по суті, формує нову конфігурацію глобального балансу сил у цифрову епоху. Саме через партнерство з демократичними державами Вашингтон прагне обмежити простір для експансії КНР, котра активно просуває власні

технологічні моделі управління інформацією, орієнтовані на централізований контроль і технологічний суверенітет [20]. Китайські ініціативи, як-от «Цифровий шовковий шлях», створюють інфраструктурні залежності у країнах Африки, Латинської Америки та Південно-Східної Азії. І це, у свою чергу, стимулює США до перегляду підходів до розвитку міжнародних цифрових стандартів і пропозиції альтернативних рішень, зокрема прозорих, сумісних і заснованих на ринкових принципах. Подібне суперництво не просто поглиблює важливість міжнародних партнерств, а й надає їм виразно геополітичного характеру [46]. Як наслідок, інформаційна безпека перестає бути лише технічним питанням і перетворюється на інструмент формування коаліцій, які захищають ліберальний порядок у світовому інформаційному просторі. Чітко простежується й тенденція до формування глобальних ініціатив, у яких США намагаються об'єднати держави з різним рівнем технічного розвитку [38]. Хорошим прикладом є ініціатива «Hyde Park Framework» 2022 року, спрямована на посилення ланцюгів постачання ІКТ і мінімізацію ризиків, пов'язаних із використанням інфраструктури, побудованої недружніми державами. Ця ініціатива передбачає, серед іншого, обмін даними про вразливості обладнання, підтримку держав у проведенні аудиту критичної інфраструктури та створення механізмів сповіщення про транснаціональні кіберінциденти. З одного боку, вона має прагматичний характер, оскільки пропонує практичні інструменти для зміцнення кіберстійкості. З іншого ж, сприяє поширенню американських стандартів безпеки та, відповідно, посиленню впливу США у цифровому просторі.

Не можна оминути увагою й роль США у створенні так званих «коаліцій за інтересами», що виникають навколо певних проблем, пов'язаних із захистом критичної інфраструктури або реагуванням на конкретні інформаційні загрози [46]. Наприклад, у 2021 році Вашингтон створив Міжнародну групу з боротьби з програмами-вимагачами (International Counter-Ransomware Initiative), до якої увійшли понад 30 держав. Ця ініціатива спрямована на координацію розвідувальних даних, взаємодію з приватним сектором, а також розробку

інструментів протидії транскордонним кримінальним мережам. Після кількох масштабних атак із застосуванням ransomware — зокрема на компанію Colonial Pipeline у США та на охоронні структури Ірландії — було очевидно, що без міжнародної взаємодії ефективно нейтралізувати подібні загрози практично неможливо. Саме завдяки роботі групи вдалося провести низку операцій із припинення діяльності мереж Maze, REvil та інших угруповань, що підтверджує дієвість коаліційного підходу. Окрему увагу заслуговує співпраця США з міжнародними фінансовими організаціями у сфері кіберзахисту [56]. Міжнародний валютний фонд та Світовий банк, маючи значні можливості впливу на політики країн, що розвиваються, активно просувають стандарти кіберстійкості у межах своїх програм, часто спираючись саме на американські рекомендації. Така взаємодія є надзвичайно важливою, оскільки руйнівні кібератаки на фінансовий сектор можуть провокувати макроекономічні кризи. Приміром, атака на Бангладеський центральний банк у 2016 році стала поштовхом до розробки глобальних стандартів банківської кібербезпеки, до створення яких залучалися й американські експерти. Відтак транснаціональні фінансові структури стають новими партнерами США у сфері інформаційної безпеки, доповнюючи політичні й військові формати.

Безумовно, міжнародне співробітництво США у сфері інформаційної безпеки не позбавлене суперечностей і складнощів. По-перше, між державами часто виникають розбіжності у трактуванні меж відповідальної поведінки акторів у кіберпросторі. Деякі держави, зокрема європейські союзники США, наполягають на більш жорстких обмеженняжених щодо діяльності спецслужб. Натомість США, маючи розгалужені розвідувальні можливості, прагнуть зберегти баланс між безпекою та конфіденційністю [20]. По-друге, іноді політичні розбіжності уповільнюють вироблення спільних рішень — як це сталося під час дискусій щодо впровадження 5G-інфраструктури, коли деякі країни опиралися обмеженням щодо обладнання Huawei, запропонованим США. По-третє, не завжди існує технічна сумісність між системами безпеки різних держав, що ускладнює оперативний обмін даними.

Попри ці виклики, США продовжують займати лідерські позиції у формуванні глобального інформаційного порядку. Важливим елементом такого лідерства є розвиток механізмів кібердипломатії, які дозволяють Вашингтону не лише реагувати на існуючі загрози, а й прогнозувати нові ризики. Наприклад, участь США у переговорах щодо штучного інтелекту в межах OECD свідчить про розуміння того, що нові технології здатні становити загрозу інформаційній стійкості, якщо вони використовуватимуться державами-суперниками для маніпуляції громадською думкою. У цьому контексті міжнародне співробітництво стає не просто інструментом реагування, а й важливим засобом формування етичних, правових та технічних рамок майбутнього цифрового світу. Варто також зауважити, що США дедалі послідовніше інтегрують питання інформаційної безпеки у власну дипломатичну стратегію. Американські посольства за кордоном відкривають спеціальні підрозділи, відповідальні за цифрову політику, а Державний департамент створив Бюро кіберпростору та цифрової політики, яке координує міжнародну діяльність США у сфері кібербезпеки, цифрових прав, розвитку інтернету та протидії дезінформації. Це демонструє еволюцію підходу, від реактивних заходів до системної, довгострокової та багаторівневої дипломатії, яка охоплює як урядові структури, так і громадянське суспільство та приватний сектор у різних країнах.

3.3. Напрямки забезпечення інформаційної безпеки США у протистоянні з КНР: досвід для України

У сучасній системі міжнародних відносин інформаційна безпека поступово перетворюється на один із ключових вимірів стратегічної конкуренції провідних центрів сили, і передусім це проявляється у протистоянні між США та КНР. Власне, ця конкуренція все більше набуває характеру довгострокового технологічного, кібернетичного та ідеологічного суперництва, що визначає глобальні тенденції розвитку цифрового простору [33]. США, реагуючи на зростання цифрового впливу КНР, сформували

комплексний багаторівневий підхід до забезпечення інформаційної безпеки, який поєднує кіберзахист, технологічне стримування, протидію дезінформації, розвиток альянсів та зміцнення стійкості критичної інфраструктури [56]. З огляду на це, аналіз американських стратегічних підходів дає можливість, по-перше, глибше зрозуміти логіку сучасної глобальної конкуренції, а по-друге, – виокремити практичні елементи, які можуть бути адаптовані Україною в умовах її власних гібридних викликів і стратегічної боротьби за свободу інформаційного простору [14].

Першим важливим напрямом є формування технологічної переваги, яка в США безпосередньо пов'язується з національною безпекою. Як свідчать події останніх років, Вашингтон систематично обмежує доступ КНР до критично важливих технологій, зокрема високопродуктивних мікрочипів і обладнання для їхнього виробництва [52]. Наприклад, у 2022-2023 роках США ухвалили низку експортних обмежень щодо китайських технологічних компаній, що, за задумом американських стратегів, має стримати розвиток обчислювального потенціалу КНР і, відповідно, її можливості у сфері штучного інтелекту та військових застосувань [45]. Це, зрештою, демонструє тісний зв'язок між інформаційною безпекою та контролем за технологічними ланцюгами. Для України подібний досвід може бути корисним у частині вибудови політики технологічного партнерства з ЄС і США, а також у формуванні власної системи контролю за критично важливими цифровими технологіями, включаючи імпорт обладнання для кіберзахисту та засобів криптографії.

Другий напрям стосується розвитку кіберстійкості та протидії кібератакам, які постають одним із найнебезпечніших інструментів сучасного гібридного протистояння. США реалізують багаторівневу федеральну систему кібербезпеки, що охоплює діяльність Агентства з кібербезпеки та безпеки інфраструктури (CISA), Кіберкомандування США, а також приватного сектору, який залучається до партнерських програм на зразок Joint Cyber Defense Collaborative [22]. Важливо зазначити, що США активно підтримують

принцип «спільної відповідальності», відповідно до якого захист цифрового середовища неможливий без координації з приватними технологічними компаніями [55]. Наприклад, під час протидії російським кібератакам у 2022 році такі корпорації, як Microsoft і Google, оперативно надавали уряду США та партнерам інформацію про шкідливі кампанії, оновлювали алгоритми виявлення загроз і підтримували критичні інфраструктурні об'єкти. Україна, яка з 2014 року перебуває в умовах інтенсивної кібероборони, могла б розширити співпрацю з американськими структурами для впровадження методологій швидкого реагування, спільного моніторингу загроз і вдосконалення стандартів стійкості державних цифрових сервісів [19].

Третім напрямом виступає протидія дезінформації та захист демократичного інформаційного простору. США, як відомо, зіткнулися з масштабними кампаніями інформаційного впливу не лише з боку КНР, а й РФ, що стало особливо помітним під час президентських виборів 2016 та 2020 років [25]. Саме тому Вашингтон активно формує політику детінізації інформаційних ланцюгів, розвиває інструменти перевірки контенту, а також підтримує діяльність Центру глобальної взаємодії (GEC), який займається виявленням і викриттям ворожих інформаційних операцій [39]. До прикладу, у 2023 році GEC опублікував аналітичні звіти про мережі китайських ботів, що поширювали прорежимні наративи в США, Південно-Східній Азії, Африці та Європі. Більше того, американські ЗМІ, аналітичні центри та ІТ-компанії активно співпрацюють задля підвищення прозорості алгоритмів соціальних мереж [16]. Для України ця практика має надзвичайне значення, оскільки протидія російській дезінформації є стратегічним пріоритетом.

Четвертий напрям – укріплення альянсів та міжнародного співробітництва у сфері цифрової безпеки. США активно використовують НАТО як платформу для координації кіберзусиль, адже з 2016 року кіберпростір офіційно визнаний окремим оперативним доменом Альянсу [33]. Власне, США підтримують розвиток натовського Центру передового досвіду з кібероборони у Таллінні, беруть активну участь у багатонаціональних

навчаннях Cyber Coalition і координують стандарти реагування на кібератаки серед союзників. Крім того, США впливають на формування глобальних стандартів безпеки 5G, обмежуючи використання китайських технологій, які можуть створювати ризики для шпигунства або контролю за інфраструктурою. Для України, що прагне поглиблення взаємодії з НАТО та інтеграції у євроатлантичний безпековий простір, американський досвід є особливо важливим.

П’ятий напрям стратегічного протистояння США та КНР полягає у розвитку системи захисту критичної інфраструктури. Американські концепції, такі як National Infrastructure Protection Plan, визначають необхідність комплексного підходу до оцінки ризиків, що охоплює енергетичні, транспортні, комунікаційні та фінансові системи [56]. США активно вдосконалюють стандарти безпеки для промислових об’єктів, що контролюються цифровими технологіями, оскільки китайські шпигунські операції неодноразово намагалися проникнути до електромереж, водних систем і телекомунікаційних вузлів [51]. Наприклад, у 2023 році ФБР та CISA офіційно повідомили про розкриття хакерських груп, пов’язаних із КНР, які прагнули встановити шкідливе програмне забезпечення у системах критичної інфраструктури Гуаму. Це стало одним із найяскравіших прикладів того, наскільки важливим є проактивний моніторинг і система раннього попередження.

Наступним напрямом є формування стратегічного наративу та ідеологічного підґрунтя інформаційної безпеки. США розглядають демократичні цінності як основу стійкості суспільства до операцій інформаційного впливу [26]. У протистоянні з КНР Вашингтон підкреслює важливість відкритості, прозорості, свободи слова та цифрових прав людини. Водночас Китай просуває альтернативну модель «керованого інформаційного суверенітету», що передбачає централізацію контролю над інтернетом і домінування державних інституцій у регулюванні комунікацій [39]. Саме

ідеологічна площина конкуренції стає дедалі важливішою, адже вона визначає, яка модель цифрової взаємодії буде визначальною у світі.

Окремої уваги потребує розвиток людського капіталу та освіти у сфері інформаційної безпеки. США системно інвестують у підготовку фахівців з кібербезпеки, державного управління, комунікацій та аналітики даних [1]. Програми університетів, наприклад у Стенфорді, Джорджтауні, MIT, розвивають кросдисциплінарний підхід, об'єднуючи технічні та гуманітарні методи аналізу. Підтримуються також численні програми підготовки співробітників державного сектору, включаючи спеціальні курси CISA та міжвідомчі тренінги [17]. Україна, яка сьогодні активно цифровізує державні послуги, може адаптувати американський досвід у розробленні навчальних програм для держслужбовців, розширенні компетенцій аналітиків інформаційних операцій, а також у створенні регіональних центрів цифрової грамотності. Зрештою, США активно формують власні глобальні коаліції для стримування китайського впливу. Йдеться про партнерства у сфері технологій (Indo-Pacific Economic Framework, Quad), коаліції щодо контролю за ланцюгами поставок, співпрацю щодо захисту від технологічного шпигунства [40]. Це підкреслює важливість створення міжнародних мереж довіри, без яких стійкість інформаційного простору неможлива. Україна, яка вже є частиною численних євроатлантичних платформ, може посилити свою участь у таких ініціативах, виступаючи не лише реципієнтом безпеки, а й рівноправним партнером, що пропонує власні інноваційні рішення, напрацьовані у ході протидії російській агресії.

Водночас важливо підкреслити, що адаптація американських підходів у сфері інформаційної безпеки не може відбуватися механічно, адже кожна держава має власну структуру загроз, інституційні можливості та політичний контекст [14]. У випадку України ключовим є врахування специфіки російських інформаційних операцій, які, на відміну від китайських, мають яскравоивно виражений деструктивний характер, спрямований на підрив державності, деморалізацію суспільства та руйнування євроінтеграційного

курсу. Саме тому деякі американські елементи — наприклад, розбудова системи стратегічних комунікацій, розширення публічно-приватного партнерства у сфері кіберзахисту, розвиток інструментів раннього виявлення кампаній впливу, мають для України навіть більшу актуальність, ніж для США [17]. Як показує практика, наявність ефективної державної інфраструктури стратегічних комунікацій демонструє свою дієвість під час криз, про що свідчить досвід України після 24 лютого 2022 року, коли швидка та скоординована комунікація уряду сприяла формуванню міжнародної підтримки та мобілізації суспільства.

Ще однією сферою, де американський досвід може бути корисним, є реформування нормативно-правової бази з питань інформаційної безпеки. У США законодавство постійно оновлюється відповідно до технологічних змін, прикладом може бути оновлена National Cybersecurity Strategy 2023 року, яка визначила нові підходи до регулювання відповідальності приватних компаній за кіберінциденти, а також запропонувала концепцію «secure-by-design» [56]. Україна, рухаючись шляхом цифровізації, має врахувати такі норми для удосконалення власних законів про кібербезпеку, інформацію та захист критичної інфраструктури [18]. Зокрема, йдеться про перегляд вимог до операторів критичної інфраструктури, розширення обов’язкових стандартів безпеки, створення механізмів звітності про інциденти й інтеграцію принципів кіберстійкості на етапі проектування державних цифрових сервісів. Не менш важливим елементом є розвиток міжвідомчої координації. США забезпечують чітку взаємодію між CISA, ФБР, Агентством національної безпеки та Пентагоном, що дозволяє швидко обмінюватися інформацією про загрози та реагувати на інциденти [22]. Україна також потребує більшої узгодженості між силами оборони, Службою безпеки України, Міністерством цифрової трансформації та Національним координаційним центром кібербезпеки при РНБО. Запровадження горизонтальних механізмів обміну інформацією, єдиних стандартів оперативного реагування й міжвідомчих центрів ситуаційного аналізу може суттєво підвищити ефективність національної

системи інформаційної безпеки. У цьому сенсі американські моделі слугують корисним орієнтиром для формування інтегрованої архітектури цифрового захисту [19].

Особливу увагу США приділяють регулюванню діяльності соціальних мереж та цифрових платформ, які дедалі більше впливають на безпековий простір. Хоча в американському суспільстві тривають дискусії щодо балансу між свободою слова та захистом користувачів, приклади запровадження обмежень щодо іноземної цифрової інфраструктури (зокрема, TikTok) вказують на прагнення мінімізувати ризики зовнішнього впливу [25]. Для України, яка стикається з масованими інформаційними операціями, питання регулювання цифрових платформ також є надзвичайно актуальним. Запровадження прозорих механізмів обмеження проросійських мереж, вимог до відкритості алгоритмів і співпраці з глобальними IT-компаніями може стати важливим елементом стратегії національної інформаційної безпеки. Американський підхід також робить акцент на інноваціях та дослідженнях, що сприяють зміцненню інформаційної переваги. Агентство передових оборонних дослідницьких проєктів DARPA, Національний науковий фонд, численні університети та приватні корпорації розвивають технології штучного інтелекту, машинного навчання, квантових комунікацій, аналізу великих даних і систем автономного виявлення загроз [42]. Наприклад, програми DARPA з автоматизації кіберзахисту дозволили створити системи, здатні самостійно знаходити та ліквідовувати вразливості у реальному часі. Для України надзвичайно цінним міг би стати розвиток власного інноваційного кластеру у сфері кіберзахисту, орієнтованого на співпрацю між державою, університетами та приватним сектором.

Важливим аспектом американської моделі є стратегічна комунікація, спрямована на формування глобального наративу щодо захисту демократичного порядку [16]. США послідовно позиціонують інформаційну безпеку як складову боротьби за свободу та відкритість міжнародного інформаційного простору, підкреслюючи, що авторитарні режими

використовують технології для контролю й обмеження людських прав. Такі меседжі спрямовані не лише на зовнішню аудиторію, а й на внутрішнє зміцнення суспільної стійкості. В Україні, де інформаційна боротьба має екзистенційний характер, розвиток стратегічних комунікацій також є важливим, особливо у сфері пояснення суспільству політики держави, боротьби з панікою, підвищення довіри до офіційних джерел і нейтралізації фейків.

Не можна оминути увагою й той факт, що протистояння США і КНР відбувається у глобальному масштабі, охоплюючи Європу, Африку, Латинську Америку та Індо-Тихоокеанський регіон [20]. Китай активно інвестує у цифрову інфраструктуру, пропонуючи дешеві технології 5G, розробляючи проєкти «Цифрового шовкового шляху» та створюючи залежність країн від своїх платформ. США, у відповідь, формують коаліції на основі безпеки ланцюгів поставок, цифрової прозорості та стандартів управління даними [46]. Для України цей аспект також має значення, адже вона поступово інтегрується у європейський та євроатлантичний простір, і її інфраструктура має відповідати стандартам безпеки союзників.

У підсумку можна стверджувати, що державна політика США у сфері інформаційної безпеки, сформована в умовах довготривалого протистояння з КНР, являє собою багаторівневу систему, де поєднуються оборонні, технологічні, політичні та ідеологічні інструменти. Україна, яка перебуває в епіцентрі глобальної гібридної боротьби та протидіє агресії держави, що широко використовує дезінформацію, кібератаки та інформаційно-психологічні операції, може адаптувати значну частину американського досвіду. Серед найбільш релевантних елементів – створення сильних міжнародних коаліцій, інвестиції у цифрові інновації, чітка міжвідомча координація, захист критичної інфраструктури, контрдезінформаційні програми та розвиток людського капіталу. Україна, інтегруючи ці підходи, здатна посилити свою цифрову стійкість, зменшити вразливість до ворожих операцій та водночас зміцнити свою позицію в євроатлантичній безпековій

архітектурі, що стає дедалі важливішим у контексті сучасної глобальної трансформації.

Висновки до розділу 3

Системний аналіз технологічного, військового та ідеологічного вимірів стратегічних підходів до інформаційної безпеки США та КНР дає змогу дійти низки узагальнених висновків, які, до речі, дозволяють не лише глибше зрозуміти характер глобального суперництва, а й окреслити практичні орієнтири для України. По-перше, інформаційна безпека дедалі більше визначається саме технологічними можливостями держав. З одного боку, Сполучені Штати продовжують зберігати лідерство в галузі штучного інтелекту, високопродуктивних обчислень, супутникових комунікацій і хмарних технологій, що стало фундаментом їхньої інформаційної переваги. З іншого боку, Китай, спираючись на політику «цифрового шовкового шляху», створює альтернативні технологічні екосистеми, які, між іншим, дозволяють Пекіну формувати власну модель глобального цифрового впливу. Саме конкуренція за стандарти ШІ, 5G та контроль над даними перетворилася на ключове поле стратегічної боротьби.

По-друге, військовий вимір є невід’ємним компонентом інформаційної потуги обох держав. Вашингтон послідовно модернізує кіберкомандування, зміцнює взаємодію розвідувальних структур і відомств оборонного сектору, а також активно застосовує концепцію «інформаційного домінування» у своїх оборонних документах. Пекін же розвиває модель «об’єднаних інформаційних операцій», у межах якої кіберзасоби, електронна війна та психологічні операції функціонують як єдиний інструмент стратегічного тиску. Відповідно, інформаційне протистояння між США та КНР поступово набуває рис довгострокового, багаторівневого конфлікту.

По-третє, міжнародне співробітництво США у сфері інформаційної безпеки, від розширення партнерств у НАТО до формування механізмів обміну даними через програми Cyber Flag і спільні кібернавчання, є важливим

ресурсом впливу на глобальні стандарти. Саме завдяки цій мережевій моделі США забезпечують не лише колективну стійкість союзників, а й глобальну підтримку власних стратегічних підходів. Зрештою, напрями забезпечення інформаційної безпеки США у протистоянні з КНР містять цінні уроки для України. Насамперед ідеться про зміцнення технологічного сектору, розвиток системи раннього виявлення кіберзагроз, розбудову партнерств із демократичними державами та формування цілісної стратегії інформаційної стійкості. Усе це, безперечно, може посилити спроможність України протидіяти зовнішнім інформаційним впливам і забезпечити власний цифровий суверенітет у довгостроковій перспективі.

ВИСНОВКИ

У результаті дослідження особливостей забезпечення інформаційної безпеки США в умовах геополітичної конкуренції з КНР, зроблено наступні висновки:

1. Розглянувши теоретичні підходи до визначення поняття «інформаційна безпека», зазначимо, що її сутність не обмежується лише захистом інформаційних ресурсів чи мережевої інфраструктури. Це комплексний феномен, який охоплює стратегічні, технологічні, військово-політичні, ідеологічні та комунікативні аспекти діяльності держав. Більше того, інформаційна безпека дедалі частіше постає як інструмент глобальної геополітичної боротьби, що визначає нову конфігурацію міжнародного суперництва. Саме тому, як показує сучасна практика, держави прагнуть досягти не лише оборонної, а й наступальної інформаційної переваги, адже контроль над інформаційними потоками, цифровими платформами та алгоритмами набуває характеру ключового ресурсу влади.

2. У цьому контексті еволюція інформаційної стратегії США демонструє фундаментальні зміни у розумінні сутності сучасного глобального протиборства. Поступово переходячи від концепції захисту критичної інфраструктури до доктрини активного стримування й формування союзницьких мереж, США визначили інформаційну перевагу одним із базових інструментів збереження лідерства у світі. Зазначимо, що стратегічні підходи США охоплюють розвиток кіберсили, боротьбу з ворожими дезінформаційними кампаніями, забезпечення технологічної домінації у сфері штучного інтелекту, квантових обчислень та мереж 5G/6G, а також консолідацію міжнародних партнерств. Власне, інформаційна політика США спрямована на формування глобального середовища, в якому демократичні країни здатні спільно протидіяти авторитарним моделям цифрового контролю, забезпечуючи захист прав особи, відкритість комунікацій та справедливі правила цифрової економіки.

3. Водночас концепція «кіберсуверенітету», розроблена КНР, відкриває протилежний за змістом підхід до формування інформаційного порядку. Підкреслюючи право держави на повний контроль над внутрішнім цифровим простором, КНР пропонує альтернативну модель світового розвитку, у якій пріоритет надається регулюванню мережі як інструменту підтримки політичної стабільності та технологічної автаркії. Політика «цифрового шовкового шляху» виходить далеко за межі економічних проєктів: вона спрямована на просування китайських цифрових стандартів у країнах Азії, Африки, Латинської Америки та навіть Європи. КНР не лише експортує телекомунікаційні технології та інфраструктуру, а й формує нову архітектуру міжнародної інформаційної взаємодії, підпорядковану логіці зміцнення його глобального впливу. Саме тому КНР активно поєднує економічні інструменти з технологічним тиском, дипломатією та інформаційними кампаніями, створюючи альтернативний центр цифрової сили.

4. Протистояння між США та КНР у сфері інформаційної безпеки проявляється не лише як конкуренція двох моделей розвитку, але й як системний конфлікт технологічних екосистем. Кіберконфлікти, що включають несанкціоновані втручання в урядові й комерційні мережі, промислове шпигунство та операції впливу, демонструють, що боротьба за інформаційну перевагу переходить у площину безперервного стратегічного суперництва. Технологічна конкуренція в галузі штучного інтелекту, напівпровідників та телекомунікаційних мереж стає вирішальним чинником для обох держав. Характерно, що цей конфлікт має також військовий вимір: інформаційні технології інтегруються у воєнні доктрини, підвищують ефективність планування операцій, забезпечують автономність бойових систем і змінюють саму природу конфлікту. Ідеологічний вимір протистояння не менш важливий, він формує глобальні наративи, впливає на міжнародні норми та визначає, яка політична модель стане визначальною в цифрову епоху.

5. Зазначено, що США активно використовують інструменти міжнародного співробітництва для посилення власних позицій у сфері

інформаційної безпеки. Зокрема, стратегічні альянси в межах НАТО, партнерство в Індо-Тихоокеанському регіоні, ініціативи «Декларації про майбутнє Інтернету» та «Партнерства з кіберстійкості» свідчать про формування глобальної мережі колективного цифрового стримування. Вашингтон прагне забезпечити стійкість демократичних держав до зовнішніх інформаційних загроз, розвиваючи стандарти обміну розвідданими, створюючи спільні підрозділи з реагування на інциденти, ініціюючи навчання та технічну підтримку партнерів. Усе це дозволяє не лише протидіяти агресивним діям КНР, а й формувати нову архітектуру безпеки, засновану на взаємній довірі та формуванні єдиних політик цифрового розвитку.

Беручи до уваги зазначене, особливо важливими є уроки для України, яка наразі перебуває у зоні підвищених кіберзагроз та є об’єктом системних інформаційних атак. Україна може використати досвід США у кількох ключових напрямах. По-перше, у розвитку національної інформаційної стратегії, що має інтегрувати військовий, дипломатичний, технологічний та комунікаційний виміри. По-друге, у створенні ефективних систем партнерств, і це стосується не лише НАТО чи ЄС, а й широкої мережі глобальних демократичних коаліцій у сфері кібербезпеки. По-третє, у посиленні технологічного потенціалу шляхом інвестицій у сферу штучного інтелекту, цифрової критичної інфраструктури та кіберстійкості державного управління. По-четверте, у вдосконаленні системи стратегічних комунікацій, здатних протидіяти іноземним інформаційним впливам, формувати позитивний міжнародний імідж держави та зміцнювати внутрішню єдність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білоусов О., Татаки Д., Татаки О. Міжнародна інформаційна безпека в США. *Філософія та політологія в контексті сучасної культури*. 2023. Т. 15, № 2. С. 82–89. DOI: https://doi.org/10.15421/352346

2. Богданьок О., Прищепа Я. На Балі завершилася зустріч лідерів США та Китаю. Що обговорили політики? *Суспільне медіа.* 2022. URL: https://suspilne.media/316010-lideri-ssa-i-kitau-14-listopada-provedut-zustric-na-bali-zmi/ (дата звернення: 03.10.2025).

3. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ». Серія: Політологія. Соціологія. Право.* 2016. № 3/4(31/32). DOI: https://doi.org/10.20535/2308-5053.2016.3/4(31/32).140496

4. Голянич Б. Зовнішні ризики безпеки Китаю: прогнози та сценарії розвитку. *Історико-політичні проблеми сучасного світу*. 2023. №48. С. 74–84. https://doi.org/10.31861/mhpi2023.48.74-84

5. Гончаренко Г. О. До проблеми визначення та розмежування дефініцій «інформаційна безпека» та «кібербезпека». *Аналітично-порівняльне правознавство.* 2024. № 5. С. 466-471. DOI:10.24144/2788-6018.2024.05.73. URL: https://app-journal.in.ua/wp-content/uploads/2024/10/75.pdf (дата звернення: 03.10.2025).

6. Копійка М. «Гостра сила» у стратегії інформаційної безпеки Китаю. *Міжнародні відносини, громадські комунікації та регіональні студії.* 2020. № 1 (7). С. 68-80. DOI: https://doi.org/10.29038/2524-2679-2020-01-68-80

7. Ланде Д. В. OSINT у кібербезпеці: навчальний посібник. Київ: ТОВ «Інжиніринг», 2024. 522 с. ISBN: 978-966-2344-97-4. URL: https://www.ipri.kiev.ua/books (дата звернення: 03.10.2025).

8. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфери: основи побудови та функціонування: монографія. Житомир: Видавець ПП «Євро-Волинь», 2021. 172 с.

9. Луценко Ю.В., Тарасюк А.В., Денисенко М.М. Кібербезпека та інформаційна безпека: разом понять. *Юридичний вісник України*. 2022. № 8. DOI: https://doi.org/10.32782/2524-0374/2022-8/70

10. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

11. Новицький В.А. Генеза поняття «інформаційна безпека»: походження та становлення. *Вчені записки ТНУ імені В.І.Вернадського. Серія: Публічне управління та адміністрування*. 2024. Том 35(74). № 4. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/06

12. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Київ: Новий світ-2000, 2023. 678 с. ISBN: 978-617-7519-44-6. URL: https://mybook.biz.ua/ua/informaciyna-bezpeka-kriptografiya/kiberbezpeka-suchasni-tehnologii-zahistu (дата звернення: 03.10.2025).

13. Остроухова В. В., Присяжнюк М. М. Інформаційна безпека. Львів: Ліра-К, 2021. 412 с. URL: https://mybook.biz.ua/ua/informaciyna-bezpeka-kriptografiya/informaciyna-bezpeka-157965/ (дата звернення: 03.10.2025).

14. Пирожик О. Про необхідність використання Україною позитивного досвіду США з питань розбудови системи інформаційної безпеки. *Вісник Пенітенціарної асоціації України.* 2021. № 2. DOI: https://doi.org/10.34015/2523-4552.2021.2.07

15. Підберезних І.Є. Політика балансування забезпечення національної безпеки США, Китаю та Країн Південно-східної Азії. *Юридична наука.* 2020. №10(112). С. 5-12. https://doi.org/10.32844/2222-5374-2020-112-10.01

16. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *Політична культура та ідеологія*. 2024. №1 (7). DOI: https://doi.org/10.53317/2786-4774-2024-1-4

17. Саранча В., Шабуніна В., Тур О. Управління інформаційною безпекою: американський досвід. *Держава та регіони. Серія: Соціальні комунікації*. 2023. № 3. DOI: https://doi.org/10.32461/2409-9805.3.2023.290991

18. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2024. №1 (41). С. 314-320. DOI: https://doi.org/10.23939/law2024.41.314

19. Стежко С.М., Шевченко Т.О. Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформаційні права та політика.* 2021. С.139-144. URL: https://doi.org/10.37750/2616-6798.2021.2(37).238349 (дата звернення: 03.10.2025).

20. Федонюк С., Магдисюк С. Протистояння між США й Китаєм у сфері кібербезпеки. *Історико-політичні проблеми сучасного світу : зб. наук. статей.* Чернівці: Чернівецький нац. ун-т, 2022. Т. 45. С. 113–127. URL: https://mhpi.chnu.edu.ua/mhpi/article/view/182

21. 2022 Report to Congress. Chapter 3: China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States. *U.S.-China Economic and Security Review Commission.* Washington, DC, 2022. URL: https://www.uscc.gov/sites/default/files/2022-11/2022_Executive_Summary.pdf (Last accessed: 03.10.2025).

22. 2023 Department of Defense Cyber Strategy: Unclassified Summary. Washington, DC: U.S. Department of Defense, 2023. 20 p. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY_SUMMARY.PDF (Last accessed: 03.10.2025).

23. Ali S. A., Amin F. Comparative Study of US-China Cyber Strategy and Its Impact on the Indo-Pacific Region. *Qlantic Journal of Social Sciences and Humanities.* 2025. №6. P. 144–157. URL: https://qjssh.com.pk/index.php/qjssh/article/download/351/385/948 (Last accessed: 03.10.2025).

24. Ali S. A., Amin F. Comparative Study of US-China Cyber Strategy and Its Impact on the Indo-Pacific Region. Qlantic Journal of Social Sciences and Humanities. 2025. Vol. 6. № 2. P. 144–157. DOI: 10.55737/qjssh.vi-ii.25351. URL: https://qjssh.com.pk/index.php/qjssh/article/download/351/385/948 (Last accessed: 03.10.2025).

25. Beijing's Global Media Influence: United States. *Freedom House.* Washington, DC: Freedom House, 2022. URL: https://freedomhouse.org/country/united-states/beijings-global-media-influence/2022 (Last accessed: 03.10.2025).

26. Biden J. R. National Security Strategy. Washington, DC : The White House, 2022. 48 p. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (Last accessed: 03.10.2025).

27. China's AI disinformation will hit lower US protection. Oxford Analytica Daily Brief. *Oxford Analytica.* 5 Sept. 2025. URL: https://www.oxan.com/insights/chinas-ai-disinformation-will-hit-lower-us-protection/ (Last accessed: 03.10.2025).

28. Chivvis C. S., Cuéllar M.-F., Medeiros E. S., Walt S. M., Culver J., Foot R., Bergsten C. F., Campanella E., Rithmire M., Fravel M. T., Heginbotham E., Perkovich G., Wong A., Wertheim S. U.S.-China Relations for the 2030s: Toward a Realistic Scenario for Coexistence. Carnegie Endowment for International Peace. 2024. URL: https://carnegieendowment.org/research/2024/10/us-china-relations-for-the-2030s-toward-a-realistic-scenario-for-coexistence?lang=en (Last accessed: 03.10.2025).

29. Comparative Study of US-China Cyber Strategy and Its Impact on Indo-Pacific Cyber Security. Quarterly Journal of Social Sciences and Humanities. 2025. URL: https://qjssh.com.pk/index.php/qjssh/article/download/351/385/948 (Last accessed: 03.10.2025).

30. Cozad M.. China's Perspective on the U.S.-China Military Balance. Santa Monica : RAND Corporation, 2023. (Research Report RRA1535-1). URL:

https://www.rand.org/pubs/research_reports/RRA1535-1.html (Last accessed: 03.10.2025).

31. Crossroads of Competition: China and Southeast Asia. *U.S.-China Economic and Security Review Commission.* Washington, DC, 2025. URL: https://www.uscc.gov/sites/default/files/2025-11/Chapter_4--Crossroads_of_Competition_China_and_Southeast_Asia.pdf (Last accessed: 03.10.2025).

32. Dar Z. A., Javid S. Navigating the Turbulent Waters: An In-Depth Study of US-China Geopolitical Rivalry. Law, *Economics and Society*. 2025. №1. URL: https://j.ideasspread.org/index.php/les/article/view/1418 (Last accessed: 03.10.2025).

33. Dimitrov D. China's Strategic Competition in Cyberspace: Implications for the United States and NATO Allies. Engineering for Rural Development. 2025. URL: https://journals.rta.lv/index.php/ETR/article/view/8618 (Last accessed: 03.10.2025).

34. Doshi R. The Long Game: China's Grand Strategy to Displace American Order. New York : Oxford University Press, 2021. 432 p. URL: https://doi.org/10.1093/oso/9780197527917.001.0001 (Last accessed: 03.10.2025).

35. Eastin A. J., Franck P. G. Restructuring Information Warfare in the United States: Shaping the Narrative of the Future. Journal of Information Warfare. 2021. Vol. 20. № 4. URL: https://fairchild-mil.libguides.com/chinese-information-warfare (Last accessed: 03.10.2025).

36. Hanson R., Grissom A. R., Mouton Ch. A. The Future of Indo-Pacific Information Warfare: Challenges and Prospects from the Rise of AI. Santa Monica : RAND Corporation, 2023. 12 p. URL: https://www.rand.org/pubs/research_reports/RRA2205-1.html (Last accessed: 03.10.2025).

37. Hanson R.. The Future of Indo-Pacific Information Warfare. Santa Monica: RAND Corporation, 2023. (Research Report RRA2205-1). URL:

https://www.rand.org/pubs/research_reports/RRA2205-1.html (Last accessed: 03.10.2025).

38. Hass R., McElveen R., McElwee L. Advancing U.S.-China Coordination amid Strategic Competition: An Emerging Playbook. *Center for Strategic and International Studies.* 2025. URL: https://www.csis.org/analysis/advancing-us-china-coordination-amid-strategic-competition-emerging-playbook (Last accessed: 03.10.2025).

39. How the People's Republic of China Seeks to Reshape the Global Information Environment. *U.S. Department of State.* Washington, DC : Global Engagement Center, 2023. 64 p. URL: https://2021-2025.state.gov/how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/ (Last accessed: 03.10.2025).

40. Indo-Pacific Strategy of the United States. Washington, DC : The White House, 2022. 19 p. URL: https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf (Last accessed: 03.10.2025).

41. Interim National Security Strategic Guidance. Washington, DC : The White House, 2021. 23 p. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/ (Last accessed: 03.10.2025).

42. Jay Johnson. U.S.-CHINA competition in emerging technologies. *Sandia National Laboratories.* 2022. C. 1–20. URL: https://www.uscc.gov/sites/default/files/2024-11/Chapter_3--U.S.-China_Competition_in_Emerging_Technologies.pdf (Last accessed: 03.10.2025).

43. Karimi M. The U.S. and China's Competition for AI Supremacy and its Implications for International Security. *Geopolitics Quarterly*. 2025. Volume: 21. № 2. P. 75-99 URL: https://journal.iag.ir/article_207240_a840ab4877be884b6c6b1d573a5a859c.pdf (Last accessed: 03.10.2025).

44. Liggett T., Helmus T. C., Grocholski K. R. How the United States Can Support Allied and Partner Efforts to Counter China in the Gray Zone: Affirmative Engagement. Santa Monica : RAND Corporation, 2024. 49 p. URL: https://www.rand.org/pubs/research_reports/RRA2954-2.html ((Last accessed: 03.10.2025).

45. Lind J., Mastanduno M. Hard Then, Harder Now: CoCom's Lessons and the Challenge of Crafting Effective Export Controls Against China. *Texas National Security Review.* 2025. №8. С. 8–33. URL: https://tnsr.org/2025/09/hard-then-harder-now-cocoms-lessons-and-the-challenge-of-crafting-effective-export-controls-against-china/ (Last accessed: 03.10.2025).

46. Liu X. Coalition Building and Sino-US Competition in the Digital Era. *The Chinese Journal of International Politics*. 2024. №17. P. 425–448. URL: https://academic.oup.com/cjip/article/17/4/425/7759853 (Last accessed: 03.10.2025).

47. Liu X. Coalition Building and Sino-US Competition in the Digital Era. *The Chinese Journal of International Politics.* 2024. Vol. 17. № 4. P. 425–448. DOI: 10.1093/cjip/poae022. URL: https://academic.oup.com/cjip/article/17/4/425/7759853 (Last accessed: 03.10.2025).

48. Malkin A., He T. The geoeconomics of global semiconductor value chains: extraterritoriality and the US–China technology rivalry. Review of International Political Economy. 2024. Vol. 31. № 2. P. 674–699. URL: https://doi.org/10.1080/09692290.2023.2284899 (Last accessed: 03.10.2025).

49. McDonagh N. US-China competition, world order and economic decoupling: insights from cultural realism. *Australian Journal of International Affairs.* 2025. №79. С. 364–384. URL: https://www.tandfonline.com/doi/full/10.1080/10357718.2025.2471353 (Last accessed: 03.10.2025).

50. Media convergence for US–China competition and disinformation in East Asia. *International Communication Gazette*. 2023. URL:

https://journals.sagepub.com/doi/10.1177/17480485231165371 (Last accessed: 03.10.2025).

51. Military and Security Developments Involving the People's Republic of China 2024: Annual Report to Congress. *U.S. Department of Defense.* Washington, DC : U.S. Department of Defense, 2024. 182 p. URL: https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF (Last accessed: 03.10.2025).

52. Miller C. Chip War: The Fight for the World's Most Critical Technology. New York : Scribner, 2022. 464 p. URL: https://books.google.com/books/about/Chip_War.html?id=JH-HEAAAQBAJ (Last accessed: 03.10.2025).

53. Molter V., DiResta R. Pandemics & propaganda: how Chinese state media creates and propagates CCP coronavirus narratives. Harvard Kennedy School Misinformation Review. 2020 (аналіз використовується у звітах 2021–2022 рр. щодо США). URL: https://cyber.fsi.stanford.edu/io/publication/pandemics-propaganda (Last accessed: 03.10.2025).

54. Naseeb J. Securitizing Cyberspace: Geopolitical Dynamics of US–China Cyber Strategic Competition. Journal of Political Stability. 2025. URL: https://journalpsa.com.pk/index.php/JPSA/article/download/195/209 (Last accessed: 03.10.2025).

55. National Cybersecurity Strategy Implementation Plan. *Office of the National Cyber Director.* Washington, DC : The White House, 2023. 57 p. URL: https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf (Last accessed: 03.10.2025).

56. National Cybersecurity Strategy. *The White House.* Washington, DC : The White House, 2023. 39 p. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (Last accessed: 03.10.2025).

57. National Cybersecurity Strategy. Washington, DC : The White House, 2023. 39 p. URL: https://www.whitehouse.gov/oncd/national-cybersecurity-strategy/ (Last accessed: 03.10.2025).

58. National Security Strategy of the United States of America. *The White House.* Washington, DC : The White House, 2022. 48 p. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата звернення: 03.12.2025).

59. Paul C. Chinese Disinformation Efforts on Social Media. Santa Monica: RAND Corporation, 2021. (Research Report RR-4373/3). URL: https://www.rand.org/pubs/research_reports/RR4373z3.html (Last accessed: 03.10.2025).

60. Riley T. Pro-Beijing operatives used social media to try promoting NYC protest. Cyberscoop. 2021 (цит. у Freedom House 2022 як приклад кампанії проти США). URL: https://cyberscoop.com/china-social-media-nyc-protest-mandiant/ (Last accessed: 03.10.2025).

61. Rura, O., Shynkaruk, N. Information Wars and Cyberwarfare in China. *Acta De Historia & Politica: Saeculum XXI*. 2023. P. 105-113. https://doi.org/10.26693/ahpsxxi2023.si.105 URL: https://ahpsxxi.org/index.php/journal/article/view/100 (Last accessed: 03.10.2025).

62. Ryan M., Burman S. Globalization, Primacy, and the US–China Tech War in «Emerging and Foundational Technologies». *The Chinese Journal of International Politics.* 2025. №18. P. 406–429. URL: https://academic.oup.com/cjip/article/18/4/406/8276066 (Last accessed: 03.10.2025).

63. Sebenius A., Carter B. Deterring Cyberattacks from Russia and China in the Era of Digital Great Power Competition. *Aspen Institute.* 2022. P. 17–19. URL: https://www.aspeninstitute.org/wp-content/uploads/2022/03/Deterring-Cyberattacks_Final.pdf (Last accessed: 03.10.2025).

64. ShevchukO., Konoplianyk, D. The information dimension of China's foreign policy strategy toward the United States in the post-cold war era. *Acta De Historia & Politica: Saeculum XX.* 2025. №09. P. 132-140. https://doi.org/10.26693/ahpsxxi2025.09.132 URL: https://ahpsxxi.org/index.php/journal/article/view/139 (Last accessed: 03.10.2025).

65. Singh N. K., Jash A., Nanjappa Y. Navigating the nexus: geopolitical, international relations and technical dimensions of US-China cyber strategic competition. *Cogent Social Sciences.* 2025. Vol. 11. № 1. URL: https://www.tandfonline.com/doi/full/10.1080/23311886.2025.2499171 (Last accessed: 03.10.2025).

66. Soriano Gatica J. P. Geopolitics in the digital age: the U.S.–China competition through their narratives on digital technologies. IDP: Revista de Internet, *Derecho y Política.* 2025. № 43. URL: https://www.researchgate.net/publication/391229778_Geopolitics_in_the_digital_age_the_US-China_competition_through_their_narratives_on_digital_technologies (Last accessed: 03.10.2025).

67. Sukumar A., Basu A. The China Gambit: Geoeconomics and the US' Turn to Informal Data Governance Initiatives. *Politics and Governance.* 2025. №13. P. 10512. URL: https://www.cogitatiopress.com/politicsandgovernance/article/download/10512/4683 (Last accessed: 03.10.2025).

68. Technology Rivalry Between the USA and China / ed. by Y. Zhang, et al. Singapore : Springer, 2023. 280 p. URL: https://content.e-bookshelf.de/media/reading/L-25038717-a90bb350e2.pdf (Last accessed: 03.10.2025).

69. Teitelbaum V. Protecting Allied Societies from Disinformation Emanating from the People's Republic of China. Brussels : NATO Parliamentary Assembly, 2025. 36 p. URL: https://www.nato-pa.int/document/2025-chinese-disinformation-report-teitelbaum-011-cdsrcs (Last accessed: 03.10.2025).

70. The Free World is Losing the Information War. Here's How It Can Win. Modern War Institute at West Point. 31 Oct. 2025. URL: https://mwi.westpoint.edu/the-free-world-is-losing-the-information-war-heres-how-it-can-win/ (Last accessed: 03.10.2025).

71. U.S.-China Economic and Security Review Commission. *U.S.-China Competition in Emerging Technologies. U.S.-China Economic and Security Review Commission Annual Report.* 2024. P. 169–197. URL: https://www.uscc.gov/sites/default/files/2024-11/Chapter_3--U.S.-China_Competition_in_Emerging_Technologies.pdf (Last accessed: 03.10.2025).

72. Vaez Mahdavi M. H., Dehshiri M. R. The Geopolitical Competition of the United States, China, and Russia in the Persian Gulf and Its Impact on the Security of the Islamic Republic of Iran. *Interdisciplinary Studies in Society, Law, and Politics.* 2025. №4. P. 1–11. URL: https://journalisslp.com/index.php/isslp/article/download/276/583/1920 (Last accessed: 03.10.2025).

73. Vuletić D. V. Concepts of Information Warfare (Operations) of the United States of America, China and Russia. *The Review of International Affairs*. 2022. №73(1185). P. 51-71. URL: https://www.researchgate.net/publication/363201937_Concepts_of_Information_Warfare_Operations_of_the_United_States_of_America_China_and_Russia (Last accessed: 03.10.2025).

74. Why the US Must Take China's Disinformation Operations Seriously. The Diplomat. 28 Jan. 2022. URL: https://thediplomat.com/2022/01/why-the-us-must-take-chinas-disinformation-operations-seriously/ (Last accessed: 03.10.2025).

75. Williams L. Force Design for the Twenty-First Century Fight: U.S. Cyber Force Lessons from China's Strategic Support Forces. Center for Strategic and International Studies, 19 November 2025. URL: https://www.csis.org/analysis/force-design-twenty-first-century-fight-us-cyber-force-lessons-chinas-strategic-support-forces (Last accessed: 03.10.2025).

76. Wolff J. The Department of Defense's Digital Logistics Are Under Attack. Brookings Institution, July 2023. URL: https://www.brookings.edu/articles/the-department-of-defenses-digital-logistics-are-under-attack/ (Last accessed: 03.10.2025).

77. Xiang N. US–China Tech War: What Chinese Tech History Reveals About Future Tech Rivalry. Singapore : World Scientific, 2021. 300 p. URL: https://www.ninaxiang.com/publications/ (Last accessed: 03.10.2025).

78. Xu M., Lu C. China-U.S. cyber-crisis management. *China Int Strategy Rev.* 2021. №3. P. 97–114. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8237537/ (Last accessed: 03.10.2025).

79. Yao Y. The New Cold War: America's new approach to Sino-American relations. *China Int Strategy Rev.* 2021. №3. P. 20–33. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8060787/ (Last accessed: 03.10.2025).

80. Zhang K. H. Geoeconomics of US–China tech rivalry and industrial policy. Journal of Asian Economics. 2024. Vol. 31. № 2. P. 674–699. URL: https://www.sciencedirect.com/science/article/pii/S2667111524000227 (Last accessed: 03.10.2025).

81. Zhao J. The Political Economy of the U.S.-China Technology War. *Monthly Review*. 2021. №73. С. 1–24. URL: https://monthlyreview.org/articles/the-political-economy-of-the-u-s-china-technology-war/ (Last accessed: 03.10.2025).

82. Zhuang A. Analysis of the Current U.S. National Security Strategy's Approach to Strategic Competition with China. In: KCAH 2024 Conference Proceedings. 2024. URL: https://papers.iafor.org/wp-content/uploads/papers/kcah2024/KCAH2024_82818.pdf (Last accessed: 03.10.2025).

АНОТАЦІЯ

Бурковський Д.А. Інформаційна безпека США в умовах геополітичної конкуренції з КНР (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 89 с. (рукопис).

Кваліфікаційна робота магістра присвячена визначенню особливості забезпечення інформаційної безпеки США в умовах геополітичної конкуренції з КНР. Об'єкт дослідження – інформаційна безпека держави в умовах геополітичної конкуренції. Предмет дослідження – механізми забезпечення інформаційної безпеки США в умовах геополітичної конкуренції з КНР.

У першому розділі розглянуто теоретичні підходи до визначення поняття «інформаційна безпека» у системі сучасних міжнародних відносин та пов'язану з нею глобальну геополітичну конкуренцію як новий вимір суперництва держав**.**

У другому розділі розкрито стратегічні підходи до забезпечення інформаційної переваги на міжнародній арені, зокрема еволюцію інформаційної стратегії США**;** визначено концепцію «кіберсуверенітету» та політику «цифрового шовкового шляху» як ключові інформаційні стратегії КНР у контексті глобального цифрового впливу.

У третьому розділі виявлено специфіку кіберконфліктів, технологічної конкуренції та боротьби за цифровий суверенітет між США та КНР, а також технологічний, військовий та ідеологічний виміри їхнього стратегічного протистояння**;** встановлено особливості міжнародного співробітництва США у сфері інформаційної безпеки та з'ясувано напрями забезпечення інформаційної стійкості у протистоянні з КНР, визначивши можливі уроки та практичне значення цього досвіду для України.

Ключові слова: інформаційна безпека США; кібербезпека; геополітична конкуренція; стратегічне суперництво США-КНР; інформаційна війна; гібридні загрози.

ANNOTATION

Burkovsky D.A. Information security of the USA in the conditions of geopolitical competition with the China (master's work). Kharkiv: V. N. Karazin Kharkiv National

University, 2025. 89 p. (manuscript).

The master's qualification work is devoted to determining the features of ensuring information security of the USA in the conditions of geopolitical competition with the China. The object of research is the information security of the state in the conditions of geopolitical competition. The subject of research is the mechanisms of ensuring information security of the USA in the conditions of geopolitical competition with the China

The first section considers theoretical approaches to defining the concept of "information security" in the system of modern international relations and the associated global geopolitical competition as a new dimension of state rivalry.

The second section reveals strategic approaches to ensuring information superiority in the international arena, in particular the evolution of the US information strategy; the concept of "cyber sovereignty" and the policy of the "digital silk road" are identified as key information strategies of the PRC in the context of global digital influence.

The third section reveals the specifics of cyber conflicts, technological competition and the struggle for digital sovereignty between the USA and the China, as well as the technological, military and ideological dimensions of their strategic confrontation; the features of US international cooperation in the field of information security are established and the directions of ensuring information stability in the confrontation with the China are clarified, identifying possible lessons and the practical significance of this experience for Ukraine.

Keywords: US information security; cybersecurity; geopolitical competition; US–China strategic rivalry; information warfare; hybrid threats.

ВІДГУК

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Бурковського Данила Андрійовича
на тему «Інформаційна безпека США в умовах геополітичної конкуренції з КНР»

1.Актуальність теми Актуальність теми інформаційної безпеки США в умовах геополітичної конкуренції з КНР зумовлена стрімким загостренням суперництва між двома провідними центрами сили, що визначають архітектуру сучасних міжнародних відносин. У міру того як Китай посилює свій технологічний, економічний та військовий потенціал, інформаційний простір стає ключовим полем боротьби за глобальне лідерство. Сполучені Штати, своєю чергою, стикаються з дедалі складнішими викликами, пов'язаними з кібершпигунством, втручанням у критичну інфраструктуру, поширенням дезінформації, а також розширенням впливу китайських цифрових платформ і телекомунікаційних компаній. Особливе значення має той факт, що конкуренція між США та КНР виходить за межі традиційної безпекової логіки, оскільки охоплює сфери штучного інтелекту, квантових технологій, космічних систем і глобальних мереж передачі даних. Усе це створює передумови для формування нових моделей інформаційної протидії, у яких стратегічні інтереси переплітаються з економічними та технологічними. Боротьба за контроль над інформаційними потоками фактично перетворюється на боротьбу за домінування у XXI столітті. Отже, дослідження даної теми є вкрай актуальним для розуміння динаміки світової політики, а також для вироблення ефективних механізмів захисту інформаційного суверенітету демократичних держав.

2. Позитивні аспекти в роботі. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Позитивними рисами кваліфікаційної роботи магістра є системність та послідовність викладення матеріалу.

3. Недоліки роботи. В той же час, автору слід було б приділити більше уваги ілюстративній частині роботи, однак це не впливає на роботу вцілому.

4. Практична цінність висновків і рекомендацій. Запропоновані у

кваліфікаційній роботі магістра теоретичні положення та висновки можуть бути використані органами влади України насамперед у формуванні більш цілісного й стратегічно виваженого підходу до забезпечення національної інформаційної безпеки, що особливо важливо в умовах посилення глобальної конкуренції між США та КНР. Досвід США, які вибудували багаторівневу систему протидії зовнішнім інформаційним впливам, дозволяє українським державним інституціям краще розуміти логіку сучасних загроз і, відповідно, адаптувати управлінські рішення; у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

5. Загальна оцінка дипломної роботи та її допуск/не допуск до захисту перед ЕК. Кваліфікаційна робота магістра Бурковського Данила Андрійовича на тему «Інформаційна безпека США в умовах геополітичної конкуренції з КНР» заслуговує на позитивну, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Керівник кваліфікаційної роботи,
кандидат політичних наук, доцент,
доцент кафедри міжнародних відносин,
міжнародної інформації та безпеки
Харківського національного

університету імені В.Н. Каразіна Пересипкіна І. В.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Бурковського Данила Андрійовича
на тему «Інформаційна безпека США в умовах геополітичної конкуренції з КНР»

1. Актуальність теми зумовлена стрімким ускладненням міжнародного середовища, де цифрові технології, штучний інтелект, великі дані та мережеві інфраструктури стають ключовими інструментами впливу на глобальний розподіл сил. З одного боку, Сполучені Штати залишаються лідером у сфері інноваційних технологій, кіберзахисту та розробки стратегій протидії дезінформаційним кампаніям. З іншого боку, Китай активно розширює свій цифровий суверенітет, інвестує у розвиток штучного інтелекту, формує альтернативні технологічні стандарти та вибудовує мережі політичного й економічного впливу через ініціативу «Цифрового шовкового шляху». У такому контексті, безпосередньо пов'язаному з формуванням нової архітектури міжнародної безпеки, інформаційне протиборство між США та КНР набуває системного характеру й охоплює як військово-політичну, так і економічну та гуманітарну площини. Більше того, загострюються ризики кібератак на критичну інфраструктуру, підвищується вразливість демократичних інституцій до іноземних інформаційних впливів, посилюється конкуренція у сфері телекомунікацій, зокрема навколо 5G і квантових технологій. Отже, всебічне вивчення цього питання дозволяє оцінити не лише стратегічні наміри обох держав, але й зрозуміти динаміку глобальної безпеки у XXI столітті.

2. Характеристика якості виконання кожного розділу роботи. У першому розділі «ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МІЖНАРОДНИХ ВІДНОСИНАХ» розглянуто теоретичні підходи до визначення поняття «інформаційна безпека» у системі сучасних міжнародних відносин та пов'язану з нею глобальну геополітичну конкуренцію як новий вимір суперництва держав.

У другому розділі «СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США ТА КНР У СУЧАСНИХ УМОВА » розкрито стратегічні підходи до забезпечення інформаційної переваги на міжнародній арені, зокрема еволюцію інформаційної стратегії США; визначено концепцію «кіберсуверенітету» та політику «цифрового шовкового шляху» як ключові інформаційні стратегії КНР у

контексті глобального цифрового впливу.

У третьому розділі «НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США У ГЕОПОЛІТИЧНОМУ ПРОТИСТОЯННІ З КНР» виявити специфіку кіберконфліктів, технологічної конкуренції та боротьби за цифровий суверенітет між США та КНР, а також технологічний, військовий та ідеологічний виміри їхнього стратегічного протистояння; встановити особливості міжнародного співробітництва США у сфері інформаційної безпеки та з'ясувати напрями забезпечення інформаційної стійкості у протистоянні з КНР, визначивши можливі уроки та практичне значення цього досвіду для України.

3. Ступінь обґрунтованості висновків роботи. Висновки достатньо обґрунтовані та відповідають поставленим завданням у кваліфікаційній роботі.

4. Використання в дипломній роботі останніх досліджень. Варто відзначити, що автором проаналізовано значний обсяг фактологічного матеріалу. Був здійснений детальний аналіз обраної проблематики, наукові методи використані коректно. Проаналізовано великий спектр вітчизняної та зарубіжної наукової літератури.

5. Позитивні сторони роботи. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. В дипломній роботі присутня системність та послідовність викладення матеріалу.

6. Недоліки роботи. Доцільно було б більше уваги приділити теоретичній частині дослідження, однак це не впливає негативно на дипломну роботу в цілому.

7. Практичне значення. Вивчення американських моделей протидії дезінформації, кіберзагрозам і технологічному впливу Китаю дозволяє українським інституціям адаптувати найефективніші практики для власної системи реагування. Водночас, впровадження принципів державно-приватного партнерства, що активно застосовуються у США для захисту критичної інфраструктури, є надзвичайно актуальним для України, яка наразі стикається з масштабними гібридними атаками.

8. Загальна оцінка кваліфікаційної роботи. Кваліфікаційна робота магістра Бурковського Данила Андрійовича на тему «Інформаційна безпека США в умовах геополітичної конкуренції з КНР» заслуговує на позитивну, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Рецензент:
кандидат політичних наук, доцент,
доцент кафедри політології,
соціології і культурології
Харківського національного педагогічного
університету імені Г. С. Сковороди КАЛЮЖНА Юлія Іванівна

Підпис [illegible]
засвідчується зав. загальним [illegible]

04. 12. 2025 р.