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: **«МІЖНАРОДНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ПОШУК ГЛОБАЛЬНИХ СТАНДАРТІВ»**

Виконав:
Студент 2-го курсу, групи УМІБ-51
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Третяк Віталій Дмитрович
(прізвище, ім'я, по батькові)

Керівник:
к.п.н., доц. Виговська Ольга Сергіївна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
к.п.н., доц. Бєлоусова Наталія Борисівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ – 2025 рік

Харківський національний університет імені В. Н. Каразіна
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин, міжнародної інформації та безпеки
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ **Н. А. Вінникова**
Підпис інніціали, прізвище

«_2_» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра
Третяк Віталія Дмитровича
(прізвище, ім'я та по батькові)

1. Тема роботи «Міжнародна політика забезпечення кібербезпеки: пошук глобальних стандартів»
керівник роботи Виговська Ольга Сергіївна, к.політ.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання студентом роботи 21 листопада 2025 року
3. Перелік питань, які потрібно розробити:

- розкрити еволюцію концепту кібербезпеки у міжнародних відносинах та теоретичні основи формування політики у цій сфері;
- виявити особливості підходів провідних держав (США, КНР) до забезпечення кібербезпеки та їх вплив на формування глобального режиму регулювання;
- охарактеризувати роль міжнародних організацій у формуванні архітектури глобальної кібербезпеки та механізми їх взаємодії;
- визначити ключові виклики міжнародного регулювання кіберпростору та перспективні шляхи формування глобальних норм і стандартів;
- обґрунтувати стратегічні пріоритети України у процесі інтеграції в глобальну систему кібербезпеки.

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 здобувачем 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	Підготовка до захисту та 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).

Студент _____ Віталій ТРЕТЯК
(підпис) (ініціали, прізвище)

Керівник роботи _____ Ольга ВИГОВСЬКА
(підпис) (ініціали, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Стрімка цифровізація всіх сфер людської діяльності у XXI столітті трансформувала кіберпростір з технічної інфраструктури у критичний домен національної та міжнародної безпеки, від якого залежить функціонування держав, економік та суспільств. Кібератаки на критичну інфраструктуру, масштабні витоки даних, дезінформаційні кампанії, кіберзлочинність та використання цифрових технологій для досягнення геополітичних цілей стали постійними елементами сучасних міжнародних відносин, підриваючи традиційні концепції суверенітету, безпеки та стабільності. За оцінками експертів, глобальні збитки від кіберзлочинності сягають сотень мільярдів доларів щорічно, а потенційні наслідки масштабних кібератак на критичну інфраструктуру можуть бути катастрофічними для життєзабезпечення мільйонів людей.

Водночас міжнародна спільнота досі не створила ефективної системи регулювання кіберпростору, здатної запобігати конфліктам, забезпечувати відповідальність за порушення та координувати глобальні зусилля у протидії кіберзагрозам. Фундаментальні розбіжності між провідними державами щодо моделі управління кіберпростором, складність атрибуції кібероперацій, відсутність універсально визнаних правових норм та механізмів їх забезпечення створюють середовище правової невизначеності та потенційної ескалації конфліктів. Транскордонна природа кіберпростору, де дії в одній юрисдикції миттєво впливають на системи в будь-якій точці світу, робить національні підходи до регулювання недостатніми без міжнародної координації та співпраці.

Для України питання кібербезпеки набуло екзистенційного значення у контексті російської агресії, яка включає не лише конвенційні військові дії, але й систематичні кібероперації проти критичної інфраструктури, державних установ, фінансового сектору та інформаційного простору. Кібератаки на українську енергетичну систему у 2015 та 2016 роках стали першими у світі випадками успішного порушення роботи електромереж через кіберзасоби, продемонструвавши реальність загроз, які раніше вважалися теоретичними. Вірус NotPetya, запущений у червні 2017 року через компрометацію

українського програмного забезпечення, завдав глобальних збитків понад 10 мільярдів доларів, ставши найдеструктивнішою кібератакою в історії. Триваюче повномасштабне вторгнення супроводжується інтенсивними кібероперaціями, спрямованими на дестабілізацію держави та суспільства.

Водночас український досвід протидії російській кіберагресії є унікальним джерелом практичних знань про природу сучасних кіберзагроз, ефективні методи захисту та механізми міжнародної співпраці в умовах реального конфлікту. Це створює можливість для України не лише зміцнити власну кіберстійкість, але й позиціонувати себе як визнаний центр експертизи у глобальних дискусіях про формування міжнародних норм та стандартів кібербезпеки. Євроінтеграційний вектор розвитку та прагнення членства в НАТО додатково актуалізують необхідність приведення національної системи кібербезпеки у відповідність до найвищих міжнародних стандартів.

У цьому контексті дослідження міжнародної політики у сфері кібербезпеки набуває особливої актуальності як для розуміння загальних закономірностей формування глобального режиму регулювання кіберпростору, так і для визначення стратегічних пріоритетів України у процесі інтеграції в євроатлантичні структури безпеки. Вивчення існуючих підходів провідних держав та міжнародних організацій, виявлення ключових викликів та можливостей міжнародної кооперації, оцінка перспектив формування ефективних глобальних норм та стандартів є необхідною інтелектуальною основою для розробки обґрунтованої національної стратегії кібербезпеки, яка враховувала б як специфічні українські умови, так і глобальні тренди цифрової трансформації міжнародних відносин.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконане у рамках наукових пріоритетів, визначених Національною стратегією кібербезпеки України, затвердженою Указом Президента України від 14 березня 2016 року № 96/2016, Законом України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року № 2163-VIII, а також Стратегією національної безпеки України, затвердженою Указом Президента України від 14 вересня 2020 року № 392/2020. Робота

узгоджується з науковими дослідженнями, що проводяться провідними українськими науковими установами у сфері інформаційної та кібернетичної безпеки, включаючи Національний інститут стратегічних досліджень, Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка та інші профільні заклади.

Мета і завдання дослідження. Метою дослідження є визначення закономірностей формування міжнародної політики у сфері кібербезпеки, виявлення ключових викликів глобального регулювання кіберпростору та обґрунтування стратегічних пріоритетів інтеграції України у міжнародну систему кіберзахисту.

Для досягнення поставленої мети визначено наступні завдання:

– розкрити еволюцію концепту кібербезпеки у міжнародних відносинах та теоретичні основи формування політики у цій сфері;

– виявити особливості підходів провідних держав (США, КНР) до забезпечення кібербезпеки та їх вплив на формування глобального режиму регулювання;

– охарактеризувати роль міжнародних організацій у формуванні архітектури глобальної кібербезпеки та механізми їх взаємодії;

– визначити ключові виклики міжнародного регулювання кіберпростору та перспективні шляхи формування глобальних норм і стандартів;

– обґрунтувати стратегічні пріоритети України у процесі інтеграції в глобальну систему кібербезпеки.

Об'єктом дослідження є міжнародна політика у сфері кібербезпеки.

Предметом дослідження є процеси формування глобальних норм та стандартів політики міжнародної кібербезпеки.

Методи дослідження. Для досягнення поставленої мети та вирішення визначених завдань у роботі застосовано комплекс загальнонаукових та спеціальних методів дослідження. Системний підхід використано для аналізу міжнародної політики кібербезпеки як складної багаторівневої системи взаємодій між різними акторами. Компаративний метод застосовано для порівняльного аналізу підходів США та Китаю до забезпечення кібербезпеки,

виявлення їх спільних рис та принципових відмінностей. Метод кейс-стаді використано для детального аналізу конкретних кіберінцидентів з міжнародними наслідками (естонські події 2007 року, Stuxnet, атаки на українську енергетику, WannaCry, Colonial Pipeline) з метою виявлення закономірностей та оцінки ефективності міжнародного реагування.

Інституційний аналіз застосовано для дослідження ролі міжнародних організацій у формуванні глобального режиму кібербезпеки. Нормативно-правовий метод використано для аналізу міжнародно-правових засад кібербезпеки, включаючи договори, конвенції, резолюції міжнародних організацій. Метод експертних оцінок залучено для інтерпретації технічних аспектів кіберзагроз та оцінки перспектив розвитку технологій. Прогностичний метод застосовано для визначення можливих сценаріїв еволюції міжнародної політики кібербезпеки та формулювання рекомендацій для України. Методологічний плюралізм дозволив забезпечити комплексність та обґрунтованість результатів дослідження.

Емпіричну базу дослідження складають офіційні документи міжнародних організацій (резолюції та звіти ООН, стратегічні концепції НАТО, директиви Європейського Союзу), національні стратегії та законодавчі акти провідних держав у сфері кібербезпеки, міжнародні договори та конвенції (Будапештська конвенція про кіберзлочинність), аналітичні звіти провідних дослідницьких центрів та організацій кібербезпеки, технічні звіти про кіберінциденти, статистичні дані міжнародних організацій (ITU Global Cybersecurity Index), матеріали міжнародних конференцій та експертних консультацій, а також наукові публікації у провідних журналах з міжнародних відносин та кібербезпеки.

Практичне значення дослідження визначається можливістю використання його результатів для формування національної стратегії кібербезпеки України, розробки рекомендацій щодо пріоритетів міжнародної співпраці, обґрунтування позицій у переговорах з міжнародними партнерами, підготовки аналітичних матеріалів для органів державної влади, а також у

навчальному процесі при викладанні дисциплін з міжнародних відносин, міжнародної безпеки та кібербезпеки у вищих навчальних закладах України.

Апробація результатів дослідження відбувалася на всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (Харків, листопад 2025 року), до якого були підготовлені тези за темою «Міжнародна політика забезпечення кібербезпеки: пошук глобальних стандартів».

Структура роботи. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 107 сторінок, з них 99 сторінок основного тексту. Список використаних джерел містить 111 найменувань.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ МІЖНАРОДНОЇ КІБЕРБЕЗПЕКИ

1.1. Поняття та еволюція концепту «кібербезпека» в міжнародних відносинах

Цифровізація фундаментально змінила природу міжнародних відносин, перетворивши кіберпростір на нову арену взаємодії між державами, корпораціями та громадянським суспільством. Кібербезпека за три десятиліття еволюціонувала від технічної проблеми захисту комп'ютерів до стратегічного пріоритету національної безпеки, що вимагає переосмислення традиційних підходів до міжнародної співпраці та глобального управління. Аналіз цієї трансформації є критично важливим для розуміння сучасних викликів глобальної безпеки та перспектив формування ефективних міжнародних механізмів кіберзахисту.

Термін «кібербезпека» має складне етимологічне походження, яке сягає грецького слова «κυβερνήτης» (kybernetes) – «кермувати» або «керманич». Американський математик Норберт Вінер використав це слово у 1948 році в своїй фундаментальній праці «Кібернетика, або Управління та зв'язок у тварині та машині» для опису науки про управління складними системами [95]. Проте сучасне розуміння кібербезпеки сформувалося значно пізніше – у 1990-х роках з появою глобального Інтернету та першими випадками комп'ютерної злочинності, які продемонстрували вразливість цифрових систем до навмисних атак.

Міжнародний союз електрозв'язку визначає кібербезпеку як «сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, керівних принципів, методів управління ризиками, дій, професійної підготовки, практичного досвіду, страхування та технологій, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувачів» [93]. Це визначення підкреслює багатовимірність феномену, який виходить далеко за межі суто технічних аспектів. Водночас у науковій літературі існують різні інтерпретації цього поняття. Джозеф Най розглядає кібербезпеку як складову «кіберсили» (cyber power) держави, що включає як захисні, так і наступальні спроможності

[101]. Мирка Данн-Кевелті акцентує увагу на процесах секьюритизації кіберзагроз, коли політичні актори конструюють певні явища як екзистенційні загрози, що виправдовує надзвичайні заходи [86].

На нашу думку, ключовою характеристикою кібербезпеки є саме її міждисциплінарність – вона одночасно є технічною проблемою (захист систем), політичною (суверенітет у кіберпросторі), економічною (захист цифрової інфраструктури), правовою (регулювання кіберпростору) та соціальною (захист прав людини онлайн). Це робить формування універсальних підходів особливо складним завданням, оскільки різні дисципліни пропонують різні методології аналізу та різні пріоритети захисту. Для України ця міждисциплінарність означає необхідність координації між технічними службами, правоохоронними органами, дипломатією та бізнесом у формуванні єдиної стратегії кібербезпеки.

Розвиток концепту кібербезпеки можна умовно поділити на чотири етапи, кожен з яких відображає зміну розуміння природи загроз та механізмів захисту. Перший етап (1990-ті – початок 2000-х) характеризувався технократичним підходом, коли кібербезпека розглядалася переважно як завдання захисту комп’ютерних систем від вірусів, несанкціонованого доступу та технічних збоїв. Основними акторами були IT-спеціалісти, а не політики чи дипломати. Характерним прикладом загроз цього періоду був вірус ILOVEYOU (2000), який завдав збитків на $10 млрд, але розглядався як технічний інцидент, а не загроза національній безпеці [108]. У цей період більшість держав ще не мали спеціалізованих урядових структур з кібербезпеки, а захист інформаційних систем покладався на внутрішні IT-відділи організацій.

Другий етап розпочався після терористичних атак 11 вересня 2001 року в США та особливо посилився після масштабних кібератак на Естонію у квітні-травні 2007 року. Естонські події стали переломним моментом, оскільки вперше продемонстрували, що координовані кібератаки можуть паралізувати функціонування цілої держави, зупинивши роботу урядових сайтів, банківської системи та медіа протягом кількох тижнів [109]. Саме після цього розпочався процес секьюритизації кіберпростору – його визнання як нового виміру національної безпеки. Держави почали створювати спеціалізовані структури

(кіберкомандування, національні центри реагування на кіберінциденти), приймати національні стратегії кібербезпеки та розглядати можливість застосування військової сили у відповідь на кібератаки. НАТО визнала кіберпростір п’ятим операційним доменом поряд з сухопутним, морським, повітряним та космічним у 2016 році [100].

Третій етап (2010-ті роки) характеризувався геополітизацією кіберпростору, коли кібероперації стали інструментом міждержавного протистояння та гібридної війни. Операція Stuxnet (2010) проти іранських ядерних об’єктів продемонструвала можливість завдання фізичної шкоди критичній інфраструктурі через кіберзасоби [111]. Втручання в американські вибори 2016 року, атаки на українську енергосистему 2015-2016 років, глобальна епідемія вірусу-здирника WannaCry у 2017 році – всі ці інциденти показали, що кіберпростір став ареною геополітичної конкуренції між великими державами [80]. У цей період сформувалися два конкуруючі підходи до управління кіберпростором: західна модель відкритого Інтернету та модель кіберсуверенітету, яку просувають Китай та Росія. Ця поляризація ускладнює формування універсальних міжнародних норм кіберповедінки.

Четвертий, сучасний етап (з 2020 року) характеризується усвідомленням кіберпростору як критичної інфраструктури всього суспільства, особливо після пандемії COVID-19, яка прискорила цифровізацію всіх сфер життя. Масовий перехід на дистанційну роботу, онлайн-освіту та цифрові послуги значно розширив поверхню потенційних атак та підвищив вразливість суспільств до кіберзагроз [88]. Водночас цей період характеризується появою нових технологій – штучного інтелекту, квантових обчислень, Інтернету речей – які одночасно створюють нові можливості для захисту та нові вразливості. Вважаємо, що цей етап вимагає переходу від суто оборонної стратегії до концепції кіберстійкості (cyber resilience), яка передбачає здатність системи не лише протистояти атакам, але й швидко відновлюватися та адаптуватися до нових загроз.

Трансформація концепту кібербезпеки тісно пов’язана з еволюцією самого кіберпростору. Якщо у 1990-х роках Інтернет був переважно інструментом

комунікації та обміну інформацією, то сьогодні він є фундаментом критичної інфраструктури, від якої залежить функціонування енергетики, транспорту, фінансової системи, охорони здоров'я та державного управління. За даними Міжнародного союзу електрозв'язку, станом на 2023 рік близько 5,3 млрд людей (66% світового населення) використовують Інтернет, а глобальна цифрова економіка становить понад $15 трлн [94]. Ця всеохоплююча цифровізація означає, що кібербезпека перестала бути периферійним питанням і стала центральним елементом національної та міжнародної безпеки.

Важливим аспектом еволюції концепту є зміна розуміння самої природи кіберзагроз. Якщо раніше основними загрозами вважалися вірусі та хакери-одинаки, то сьогодні спектр загроз включає державні кібероперації, організовані злочинні групи, кібертероризм, промислове шпигунство та дезінформаційні кампанії. Бенджамін Бьюкенен у своїй праці «The Hacker and the State» показує, як держави інтегрували кіберспроможності у свої стратегії національної безпеки, створивши нову реальність «кіберперсистенції» (cyber persistence), де конфлікт у кіберпросторі є постійним та розгортається нижче порогу відкритої війни [82]. Це вимагає переосмислення традиційних концепцій миру та війни, оскільки кіберпростір характеризується постійною конфліктністю без формального оголошення воєнних дій.

Концепція кіберсуверенітету стала одним із найбільш дискусійних аспектів сучасного розуміння кібербезпеки. Вона передбачає право держави контролювати інформаційні потоки на своїй території та встановлювати правила функціонування Інтернету в межах національної юрисдикції. Китай активно просуває цю концепцію через ініціативи на міжнародних платформах, аргументуючи необхідністю захисту національної безпеки та культурної ідентичності [107]. Водночас критики вказують, що кіберсуверенітет може використовуватися для виправдання цензури, порушення прав людини та фрагментації глобального Інтернету. На нашу думку, для України оптимальним є європейський підхід, який балансує між захистом суверенітету (через регулювання критичної інфраструктури) та збереженням відкритості

кіберпростору (через захист прав людини та свободи інформації), що відповідає вимогам інтеграції до Європейського Союзу.

Еволюція концепту кібербезпеки також відображається у формуванні спеціалізованої термінології. Поняття «кібератака», «кіберінцидент», «кіберзлочин», «кібервійна», «кібертероризм», «кіберстійкість» мають різні значення залежно від контексту та правової системи. Відсутність універсально прийнятих визначень створює додаткові виклики для міжнародної співпраці. Наприклад, Таллінське керівництво з міжнародного права, застосовного до кібероперацій, пропонує детальний аналіз правових аспектів кібервійни, але визнає, що багато концепцій залишаються дискусійними навіть серед експертів [104]. Проблема атрибуції – встановлення джерела кібератаки – залишається однією з найскладніших технічних та правових проблем, оскільки анонімність та можливість маскування у кіберпросторі дозволяють зловмисникам приховувати свою ідентичність.

Розвиток концепту кібербезпеки у контексті міжнародних відносин супроводжується формуванням нових форм міждержавної взаємодії та конфлікту. З одного боку, спостерігається зростання міжнародної співпраці через двосторонні та багатосторонні угоди про обмін інформацією про кіберзагрози, створення регіональних центрів реагування на кіберінциденти, спільні навчання та операції проти кіберзлочинності [105]. З іншого боку, кіберпростір стає ареною міждержавного протистояння, де держави використовують кібероперації для шпигунства, саботажу, впливу на вибори та досягнення інших стратегічних цілей без застосування традиційної військової сили. Це створює парадоксальну ситуацію, коли держави одночасно співпрацюють у боротьбі з кіберзлочинністю та конкурують у розвитку наступальних кіберспроможностей.

Вважаємо, що концепт кібербезпеки продовжує еволюціонувати під впливом технологічних інновацій та геополітичних трансформацій. Поява штучного інтелекту створює принципово нові виклики, оскільки ШІ може використовуватися як для автоматизації кібератак (генерація шкідливого коду, фішинг, аналіз вразливостей), так і для захисту (виявлення аномалій,

прогнозування загроз, автоматизоване реагування). Квантові обчислення загрожують зробити неефективними сучасні криптографічні методи, що вимагає розробки постквантової криптографії [99]. Інтернет речей розширює поверхню атак, оскільки мільярди підключених пристроїв часто мають слабкий захист і можуть використовуватися для створення потужних ботнетів. Ці технологічні зміни вимагають постійної адаптації концептуальних підходів до кібербезпеки.

Український досвід є унікальним вкладом у глобальне розуміння кібербезпеки. З 2014 року Україна стала «полігоном» для випробування найсучасніших кіберзброї та тактик гібридної війни, зазнавши понад десяти масштабних кібератак, включаючи першу у світі успішну атаку на енергосистему (2015), вірус NotPetya (2017), який завдав глобальних збитків на $10 млрд, та постійні атаки на державні установи і критичну інфраструктуру [91]. Цей трагічний досвід водночас сформував унікальну експертизу протидії кіберзагрозам в умовах активного конфлікту, розвитку кіберстійкості та ефективного публічно-приватного партнерства. На наше переконання, український досвід має стати основою для створення регіонального центру компетенції з кібербезпеки, який міг би ділитися практичними знаннями з країнами, що стикаються з подібними викликами.

Таким чином, еволюція концепту кібербезпеки відображає фундаментальну трансформацію міжнародних відносин в епоху цифровізації. Від суто технічного поняття кібербезпека перетворилася на комплексний феномен, який охоплює політичні, економічні, соціальні та військові аспекти функціонування сучасних держав. Ця трансформація вимагає нових теоретичних підходів до аналізу міжнародної безпеки, нових правових інструментів регулювання та нових форм міжнародної співпраці. Для України розуміння цієї еволюції є критично важливим для формування ефективної національної стратегії кібербезпеки та успішної інтеграції в європейські та євроатлантичні структури кіберзахисту. Подальший аналіз теоретичних підходів до формування політики кібербезпеки дозволить глибше зрозуміти, які концептуальні рамки є найбільш придатними для пояснення та вирішення сучасних викликів у цій сфері.

1.2. Теоретичні підходи до формування політики у сфері кібербезпеки

Формування ефективної політики кібербезпеки вимагає глибокого теоретичного осмислення природи кіберпростору, специфіки кіберзагроз та механізмів забезпечення безпеки в умовах цифрової трансформації суспільства. Складність та багатовимірність феномену кібербезпеки, який поєднує технологічні, політичні, економічні, соціальні та культурні аспекти, породжує різноманітність теоретичних перспектив для його аналізу. На нашу думку, жоден із існуючих підходів не здатен самостійно охопити всю складність кібербезпеки, що вимагає синтезу різних методологічних інструментів для розуміння та вирішення практичних проблем кіберзахисту на національному та міжнародному рівнях.

Теоретичне підґрунтя політики кібербезпеки формується на перетині класичних теорій міжнародних відносин, концепцій стратегічних досліджень та специфічних підходів, розроблених для аналізу цифрового середовища. Основні теоретичні школи міжнародних відносин – реалізм, лібералізм та конструктивізм – пропонують різні інтерпретації природи кіберзагроз, ролі держави в забезпеченні кібербезпеки та оптимальних стратегій міжнародної співпраці. Кожен із цих підходів акцентує увагу на різних аспектах кібербезпеки та має різні імплікації для формування національної та міжнародної політики, що робить їх порівняльний аналіз критично важливим для розробки збалансованих стратегій кіберзахисту.

Реалістична парадигма розглядає кіберпростір як нову арену міждержавної конкуренції та боротьби за владу, де держави залишаються центральними акторами, а головною метою є максимізація національної безпеки через нарощування кіберспроможностей та створення систем стримування. Джозеф Най, один із провідних теоретиків кібербезпеки, адаптував реалістичні концепції до цифрового середовища, вказуючи на парадокс кібервразливості: технологічно розвинені держави стають більш уразливими до кібератак саме через високий рівень цифровізації їхніх економік та критичної інфраструктури [102]. Це

створює асиметричну ситуацію, коли менш розвинені держави або недержавні актори можуть завдати непропорційної шкоди потужним державам з мінімальними інвестиціями в кіберзброю. Реалісти підкреслюють, що анархічна природа міжнародної системи та відсутність глобального регулятора роблять кіберпростір середовищем самодопомоги, де держави змушені розраховувати на власні сили для захисту національних інтересів.

Неореалістична інтерпретація кібербезпеки акцентує увагу на структурних характеристиках кіберпростору та їх впливі на поведінку держав. Брендон Валеріано та Райан Майнесс у своїх дослідженнях показують, що попри зростання кількості кіберінцидентів між державами, більшість із них залишаються нижче порогу відкритого конфлікту та використовуються переважно для шпигунства, а не деструктивних атак [110]. Це пояснюється раціональними розрахунками держав, які усвідомюють ризики ескалації та невизначеність наслідків масштабних кібероперацій. Водночас реалісти визнають обмеженість традиційних механізмів стримування у кіберпросторі через складність атрибуції, низький поріг входження для різних акторів та проблематичність демонстрації кіберспроможностей без їх фактичного використання, що створює дилему безпеки в цифровому середовищі [81].

Ліберальна парадигма пропонує альтернативний погляд на формування політики кібербезпеки, наголошуючи на важливості міжнародної співпраці, створення режимів та інституцій для управління кіберпростором, а також розвитку норм відповідальної поведінки держав у цифровому середовищі. Прихильники лібералізму вважають, що спільні економічні вигоди від стабільного та безпечного кіберпростору створюють стимули для кооперації навіть між державами-суперниками, оскільки взаємозалежність цифрових систем означає, що кібератаки можуть мати непередбачувані колатеральні наслідки для країни-агресора та її союзників [103]. Інституціональний підхід підкреслює роль міжнародних організацій, таких як Група урядових експертів ООН, Міжнародний союз електрозв'язку та регіональні структури, у формуванні правил гри у кіберпросторі та забезпеченні платформ для діалогу між різними стейкхолдерами.

Ліберали особливо акцентують увагу на ролі недержавних акторів у забезпеченні кібербезпеки. Оскільки більшість критичної цифрової інфраструктури належить приватним компаніям, а технологічні корпорації контролюють глобальні платформи комунікації та обміну даними, ефективна політика кібербезпеки неможлива без активного залучення бізнесу до процесів регулювання та стандартизації [83]. Публічно-приватне партнерство розглядається як оптимальна модель, яка поєднує регуляторні можливості держави з технологічною експертизою та ресурсами приватного сектору. Розвиток ліберального підходу супроводжується формуванням концепції кібердипломатії як специфічного напряму зовнішньополітичної діяльності держав, спрямованого на врегулювання кіберконфліктів через дипломатичні канали та багатосторонні переговори замість силових методів [79].

Конструктивістський підхід фокусується на процесах соціального конструювання кіберзагроз, ролі дискурсу та наративів у формуванні сприйняття кібербезпеки, а також впливі норм, ідентичностей та культурних факторів на кіберповедінку держав та інших акторів. Мирка Данн-Кевелті розглядає кібербезпеку як результат політичного процесу секьюритизації, коли певні явища конструюються політичними елітами як екзистенційні загрози, що легітимізує надзвичайні заходи та перерозподіл ресурсів [87]. Конструктивістська перспектива дозволяє аналізувати різноманітність національних підходів до кібербезпеки через призму культурних особливостей, історичного досвіду та домінуючих політичних дискурсів у різних країнах, що пояснює, чому одні держави акцентують увагу на кіберсуверенітеті та контролі над інформаційними потоками, тоді як інші пріоритизують відкритість кіберпростору та захист прав людини в цифровому середовищі.

Конструктивісти також досліджують процеси формування кібернорм як неформальних правил поведінки у кіберпросторі, які виникають через соціалізацію, навчання та дифузію між державами та іншими акторами. Епістемічні спільноти експертів з кібербезпеки відіграють важливу роль у формуванні спільного розуміння природи кіберзагроз та оптимальних стратегій кіберзахисту, впливаючи на національні політики через консультації,

дослідження та міжнародні конференції [89]. На нашу думку, конструктивістський підхід особливо корисний для розуміння того, чому міжнародна співпраця у сфері кібербезпеки часто буксує попри об'єктивні спільні інтереси – різні культурні та ідеологічні контексти призводять до фундаментально різного розуміння того, що саме потрібно захищати і якими методами це робити.

Для систематизації та порівняння розглянутих теоретичних підходів нами розроблено таблицю 1.1, яка демонструє ключові відмінності між реалізмом, лібералізмом та конструктивізмом у контексті кібербезпеки, а також оцінює їх релевантність для української політики в цій сфері.

Таблиця 1.1

Порівняння теоретичних підходів до кібербезпеки

Підхід	Ключові актори	Природа загроз	Механізми захисту	Релевантність для України
Реалізм	Держави як унітарні раціональні актори	Міждержавна конкуренція, боротьба за владу в кіберпросторі	Нарощування кіберспроможностей, стримування, балансування	Висока – враховує російську загрозу та необхідність розвитку власних спроможностей
Лібералізм	Держави + недержавні актори (корпорації, НУО, міжнародні організації)	Транснаціональні загрози, кіберзлочинність, вразливості системи	Міжнародне співробітництво, режими, інституції, публічно-приватне партнерство	Середня – потребує довіри між акторами, яка наразі обмежена; важлива для євроінтеграції
Конструктивізм	Всі стейкхолдери через соціальні процеси	Соціально сконструйовані, залежать від дискурсу та ідентичності	Формування норм, зміна дискурсу, створення спільних значень	Середня – корисна для розуміння міжнародних розбіжностей, але має довгостроковий ефект

Джерело: складено автором на основі [102; 103; 87]

Як видно з таблиці 1.1, кожен теоретичний підхід має свої сильні та слабкі сторони в застосуванні до аналізу кібербезпеки. Для України оптимальним є

синтез реалістичного та ліберального підходів: реалізм пояснює необхідність розвитку власних кіберспроможностей для протидії державним агресорам, особливо в умовах триваючої гібридної війни з Росією, тоді як лібералізм обґрунтовує важливість міжнародної співпраці та інтеграції в євроатлантичні структури кібербезпеки. Конструктивістська перспектива доповнює цей синтез, пояснюючи, чому Україна має активно працювати над зміною міжнародного дискурсу щодо кібернорм, використовуючи власний досвід як аргумент для посилення міжнародних механізмів відповідальності за кібератаки.

Теорія комплексної взаємозалежності, розроблена Робертом Кеохейном та Джозефом Наєм, надає важливі інсайти для розуміння політики кібербезпеки в умовах глобалізації. Кіберпростір створює безпрецедентний рівень взаємозалежності між державами, корпораціями та індивідами, що одночасно генерує нові можливості для співпраці та нові вразливості [96]. Концепція мережевої безпеки підкреслює, що у взаємопов'язаному кіберпросторі безпека кожного актора залежить від безпеки всієї системи, що вимагає колективних підходів до забезпечення кіберстійкості. Парадокс взаємозалежності полягає в тому, що спроби окремих держав забезпечити свою кібербезпеку через унілатеральні заходи, такі як створення національних сегментів Інтернету або накопичення кіберзброї, можуть підривати загальну стабільність кіберпростору та створювати нові ризики для всіх учасників цифрової екосистеми.

Теорія стійкості (resilience theory) набуває дедалі більшого значення у формуванні сучасної політики кібербезпеки. Вона визнає неможливість повного запобігання кібератакам та акцентує увагу на здатності систем адаптуватися, відновлюватися та продовжувати функціонування в умовах постійних кіберзагроз [98]. Концепція кіберстійкості включає технічні, організаційні та соціальні виміри: резервування критичних систем, розробку планів безперервності бізнесу, навчання персоналу та формування культури кібербезпеки на всіх рівнях суспільства. Український досвід протидії масштабним кібератакам на енергетичну інфраструктуру (2015-2016) та швидкого відновлення після вірусу NotPetya (2017) демонструє практичну цінність підходу, заснованого на стійкості, коли пріоритетом є не лише

запобігання атакам, але й мінімізація їх наслідків та швидке відновлення функціональності [92].

Підхід, заснований на управлінні ризиками, пропонує систематичну методологію для ідентифікації, оцінки та пріоритизації кіберзагроз, а також розробки пропорційних заходів кіберзахисту з урахуванням наявних ресурсів та прийнятного рівня ризику для організації чи держави. Ризик-орієнтована політика кібербезпеки передбачає постійний моніторинг загроз, регулярне оновлення оцінок ризиків та адаптацію захисних заходів відповідно до змін у ландшафті кіберзагроз, що забезпечує динамічний та проактивний підхід до кіберзахисту замість статичних та реактивних моделей безпеки [90]. Цей підхід особливо актуальний для ресурсно-обмежених країн, які не можуть забезпечити максимальний захист усім системам одночасно і повинні стратегічно розподіляти кошти на основі об'єктивної оцінки загроз та потенційних збитків.

Теорія публічно-приватного партнерства у сфері кібербезпеки визнає критичну роль приватного сектору у забезпеченні кіберзахисту, оскільки більшість критичної інфраструктури та цифрових сервісів належить та управляється приватними компаніями. Це вимагає нових моделей співпраці між державою та бізнесом, які поєднували б регуляторні можливості та розвідувальні спроможності держави з технологічною експертизою та інноваційним потенціалом приватного сектору [106]. Успішні моделі такої співпраці включають створення галузевих центрів обміну інформацією про загрози (Information Sharing and Analysis Centers), спільні навчання та симуляції кібератак, розробку індустріальних стандартів кібербезпеки за участю державних регуляторів та приватних компаній, а також механізми координованого розкриття вразливостей. Вважаємо, що для України розвиток публічно-приватного партнерства є критично важливим, оскільки держава не має достатніх ресурсів для забезпечення кібербезпеки самостійно, а потужний сектор ІТ-індустрії (понад 200 тисяч спеціалістів) може стати стратегічним партнером у зміцненні національної кіберстійкості.

Мультистейкхолдерний підхід до управління кіберпростором пропонує альтернативу традиційній міждержавній моделі управління, залучаючи до

процесів прийняття рішень представників приватного сектору, громадянського суспільства, технічної спільноти та академічних кіл. Цей підхід базується на принципах інклюзивності, прозорості та підзвітності, визнаючи, що ефективна політика кібербезпеки повинна враховувати інтереси та експертизу різних груп стейкхолдерів, які мають унікальні перспективи та ресурси для вирішення проблем кіберзахисту [85]. Практична реалізація мультистейкхолдерної моделі демонструє як переваги, так і виклики: залучення множинних акторів сприяє легітимності та ефективності політичних рішень, але водночас ускладнює процеси координації та може призводити до розмивання відповідальності. Балансування між різними інтересами стейкхолдерів вимагає розробки механізмів консенсусу та компромісу, що може уповільнювати прийняття рішень в умовах швидкої еволюції кіберзагроз.

Критичні дослідження безпеки (Critical Security Studies) пропонують альтернативну перспективу на формування політики кібербезпеки, ставлячи під сумнів домінуючі дискурси та практики кіберзахисту, особливо їх вплив на права людини, приватність та демократичні свободи. Представники критичного підходу аналізують, як політика кібербезпеки може використовуватися для легітимізації цифрового нагляду, цензури Інтернету та обмеження громадянських свобод під приводом боротьби з кіберзагрозами [84]. На нашу думку, цей підхід є особливо важливим для демократичних суспільств, які прагнуть збалансувати вимоги безпеки із захистом фундаментальних прав. Українська практика показує можливість ефективного кіберзахисту без жертвування демократичними цінностями: попри масштабні кіберзагрози, Україна зберігає відкритий Інтернет та не запроваджує тотального цифрового нагляду, на відміну від деяких сусідніх країн.

Порівняльний аналіз розглянутих теоретичних підходів показує, що формування ефективної політики кібербезпеки вимагає еклектичного підходу, який інтегрує елементи різних теоретичних традицій залежно від специфічного контексту та викликів, з якими стикається держава. Для України, яка одночасно протистоїть агресивним кібероперaціям державного рівня та прагне інтегруватися в європейські та євроатлантичні структури, оптимальною є

комбінація реалістичного визнання загроз, ліберального акценту на міжнародній співпраці та інституційному розвитку, конструктивістського розуміння важливості норм та дискурсу, а також прагматичного фокусу на стійкості та управлінні ризиками. Такий синтетичний підхід дозволяє розробляти політику, яка є водночас реалістичною щодо загроз, амбітною щодо міжнародної співпраці та прагматичною щодо використання обмежених ресурсів.

Важливим аспектом теоретичного осмислення кібербезпеки є визнання динамічної природи як самого кіберпростору, так і теоретичних підходів до його аналізу. Поява нових технологій, таких як штучний інтелект, квантові обчислення та блокчейн, вимагає постійної адаптації існуючих теорій та розробки нових концептуальних рамок. Теоретичні дебати про застосовність традиційних концепцій стримування до кіберпростору, про межі кіберсуверенітету, про баланс між безпекою та приватністю залишаються відкритими та продовжують еволюціонувати разом з технологічними та геополітичними змінами [97]. Для практиків політики кібербезпеки це означає необхідність постійного інтелектуального оновлення та готовності переглядати усталені підходи у світлі нових викликів та можливостей.

Таким чином, теоретичні підходи до формування політики кібербезпеки представляють багатий інструментарій для аналізу та вирішення складних проблем захисту в цифровому середовищі. Кожен із розглянутих підходів – від традиційних теорій міжнародних відносин до специфічних концепцій, розроблених для цифрового контексту – вносить унікальний внесок у наше розуміння природи кіберзагроз та оптимальних стратегій протидії їм. Для України ефективна політика кібербезпеки має базуватися на синтезі цих підходів, враховуючи специфічний контекст гібридної війни, обмеженість ресурсів та стратегічний вектор євроатлантичної інтеграції. Розглянуті теоретичні підходи створюють концептуальну основу для аналізу міжнародно-правових механізмів забезпечення кібербезпеки, які формують нормативну базу для регулювання поведінки держав та інших акторів у кіберпросторі.

1.3. Міжнародно-правові засади забезпечення кібербезпеки

Формування міжнародно-правових засад забезпечення кібербезпеки являє собою один із найскладніших викликів сучасного міжнародного права, оскільки традиційні правові концепції та норми, розроблені для фізичного простору, часто виявляються недостатніми або неадекватними для регулювання відносин у кіберпросторі, який характеризується транскордонністю, анонімністю, швидкістю поширення інформації та складністю атрибуції дій. Еволюція міжнародно-правового регулювання кібербезпеки відбувається через адаптацію існуючих норм міжнародного права до специфіки кіберпростору, розробку нових правових інструментів та формування звичаєвого права через практику держав і рішення міжнародних організацій. На нашу думку, ефективність міжнародно-правового регулювання кібербезпеки залежить не стільки від створення нових договорів, скільки від досягнення консенсусу щодо інтерпретації існуючих норм та розробки практичних механізмів їх застосування в умовах цифрової реальності, що особливо актуально для України в контексті протидії російській кіберагресії.

Фундаментальне питання застосовності міжнародного права до кіберпростору було предметом тривалих дискусій у міжнародній спільноті протягом 2000-х років. Консенсус, досягнутий у рамках Групи урядових експертів ООН з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки у 2013 та 2015 роках, підтвердив, що міжнародне право, зокрема Статут ООН у повному обсязі, застосовується до кіберпростору. Це рішення створило правову основу для регулювання кіберопераційної та відповідальності держав за кібердіяльність, хоча залишило відкритими багато питань щодо конкретної інтерпретації та застосування окремих правових норм. Як зазначає О. Баранов, українське законодавство про кібербезпеку формувалося саме з урахуванням цих міжнародних напрацювань, хоча адаптація глобальних норм до національного контексту відбувалася з певними труднощами через новизну проблематики та відсутність усталеної юридичної практики [2].

Принцип суверенітету як основоположний принцип міжнародного права поширюється на кіберінфраструктуру, розташовану на території держави, та

кібердіяльність, яка здійснюється з її території або під її юрисдикцією, що надає державам суверенні права щодо регулювання кіберпростору, але також покладає на них обов’язки щодо запобігання використанню їхньої території для шкідливої кібердіяльності проти інших держав. Застосування принципу суверенітету до кіберпростору породжує складні правові питання щодо меж державної юрисдикції в транскордонному цифровому середовищі, екстратериторіального застосування національного законодавства та конфлікту юрисдикцій у випадках, коли кіберопераційна зачіпає території та інтереси множинних держав. Концепція кіберсуверенітету, яка активно просувається деякими державами, передбачає розширене тлумачення суверенних прав у кіберпросторі, включаючи право контролювати інформаційні потоки та регулювати діяльність інтернет-платформ на національній території. Це викликає занепокоєння щодо фрагментації глобального кіберпростору та обмеження основних прав і свобод людини в цифровому середовищі [16].

Вважаємо, що для України оптимальним є європейське розуміння кіберсуверенітету, яке визнає право держави захищати критичну інфраструктуру та регулювати цифровий ринок, але не дозволяє використовувати суверенітет як виправдання для цензури або порушення прав людини онлайн. Український законодавець у Законі "Про основні засади забезпечення кібербезпеки України" від 2017 року спробував збалансувати ці підходи, закріпивши як суверенні права України у кіберпросторі, так і гарантії прав і свобод громадян у цифровому середовищі [30]. Водночас практична реалізація цього балансу залишається складним завданням, особливо в умовах триваючого збройного конфлікту та гібридної війни, коли вимоги безпеки часто вступають у конфлікт з гарантіями свободи інформації.

Міжнародне гуманітарне право, також відоме як право збройних конфліктів, застосовується до кіберопераційна, які проводяться у контексті збройного конфлікту, що означає необхідність дотримання принципів розрізнення між військовими та цивільними об’єктами, пропорційності, запобігання надмірним стражданням та вжиття запобіжних заходів при плануванні та проведенні кібератак. Таллінське керівництво з міжнародного

права, застосовного до кібервійни, розроблене групою провідних експертів під егідою Центру передового досвіду НАТО з питань спільної кіберзахисту, представляє найбільш комплексний аналіз застосування міжнародного гуманітарного права до кібероперацийна. Хоча це керівництво не є офіційним документом і відображає експертні думки, а не узгоджені позиції держав, воно стало важливим довідковим інструментом для військових юристів, політиків та науковців. В. Ліпкан підкреслює, що українська доктрина кібербезпеки повинна враховувати положення міжнародного гуманітарного права, особливо в контексті захисту цивільної критичної інфраструктури від кібератак під час збройного конфлікту [47].

Визначення порогу, при перевищенні якого кібероперацийна можуть кваліфікуватися як застосування сили або збройний напад у розумінні статей 2(4) та 51 Статуту ООН, залишається одним із найбільш дискусійних питань міжнародного права кібербезпеки. Більшість кібератак не завдають фізичної шкоди, але можуть мати серйозні економічні, соціальні та політичні наслідки, що ускладнює їх правову кваліфікацію. Критерії оцінки кібероперацийна включають масштаб наслідків, безпосередність ефекту, прямоту причинно-наслідкового зв’язку, інвазивність, вимірність наслідків, військовий характер та залучення державних акторів. Проте відсутність універсально визнаних критеріїв створює правову невизначеність та ризики ескалації кіберконфліктів. На нашу думку, ключовою прогалиною міжнародного кіберправа є саме ця невизначеність порогів: навіть якщо технічно доведено державне походження атаки та її серйозні наслідки, політичні міркування часто перешкоджають кваліфікації інциденту як застосування сили, що підриває ефективність правових механізмів [11].

Право на самооборону, закріплене у статті 51 Статуту ООН, може бути реалізоване у відповідь на кібератаки, які досягають рівня збройного нападу, при цьому держави мають право використовувати як кінетичні, так і кіберзасоби для самооборони, дотримуючись принципів необхідності, пропорційності та безпосередності. Превентивна самооборона у кіберпросторі викликає особливі суперечності через складність встановлення неминучості кібератаки та ризики

помилкової атрибуції, що може призвести до непропорційних відповідних дій проти невинних сторін або ескалації конфлікту на основі хибних припущень. Український досвід протидії російським кібератакам з 2014 року демонструє практичні складнощі застосування права на самооборону: попри численні документовані атаки з боку Росії, включаючи NotPetya та атаки на енергосистему, жодна з них не була офіційно кваліфікована як збройний напад, що дозволило б застосувати право на самооборону у повному обсязі. М. Ожеван зазначає, що це створює правовий вакуум, коли держава-жертва не може адекватно відповісти на системні кібератаки через відсутність чіткої правової кваліфікації таких дій у міжнародному праві [65].

Проблема атрибуції кібероперацийна до конкретних держав або недержавних акторів створює фундаментальні виклики для застосування міжнародного права, оскільки встановлення відповідальності держави вимагає доказів того, що кібероперацийна була здійснена державними органами або особами, які діяли за вказівками, під керівництвом або контролем держави. Стандарти доказування для атрибуції кібератак варіюються залежно від контексту та потенційних наслідків атрибуції, від технічної до політичної. Політичні міркування часто впливають на публічну атрибуцію кібератак: навіть за наявності технічних доказів причетності певних акторів, держави можуть утримуватися від публічного звинувачення через дипломатичні, економічні або стратегічні міркування. Технічна атрибуція рідко надає абсолютну впевненість у державному походженні атаки, що залишає простір для правдоподібного заперечення з боку держав-агресорів. Досвід України показує, що навіть детальна технічна документація кібератак та їх атрибуція міжнародними експертами не завжди призводять до адекватної міжнародно-правової відповіді через політичні чинники [23].

Міжнародне право прав людини залишається повністю застосовним у кіберпросторі, що означає зобов’язання держав поважати та захищати права людини в цифровому середовищі, включаючи право на приватність, свободу вираження поглядів, свободу асоціацій та доступ до інформації. Резолюції Ради ООН з прав людини підтверджують, що права, які людина має офлайн, повинні

також захищатися онлайн. Це створює правові обмеження для державних заходів кібербезпеки, які можуть порушувати права людини під приводом забезпечення національної безпеки. Балансування між вимогами кібербезпеки та захистом прав людини представляє складну правову та етичну дилему, оскільки заходи кіберзахисту можуть одночасно захищати від кіберзагроз та створювати ризики для приватності та інших основних прав. Принцип пропорційності вимагає, щоб обмеження прав людини з міркувань кібербезпеки були передбачені законом, переслідували легітимну мету та були необхідними та пропорційними в демократичному суспільстві.

Вважаємо, що Україна, попри масштабні кіберзагрози з боку росії, повинна дотримуватися високих стандартів захисту прав людини онлайн, оскільки це не лише міжнародно-правовий обов'язок, але й стратегічне питання ідентичності: на відміну від авторитарних сусідів, Україна позиціонує себе як демократична держава, де кібербезпека забезпечується без жертвування фундаментальними свободами. Український Закон "Про захист персональних даних" та його подальша адаптація до вимог GDPR демонструють прагнення країни дотримуватися європейських стандартів балансу між безпекою та приватністю [29].

Будапештська конвенція про кіберзлочинність 2001 року залишається єдиним універсальним міжнародним договором, спеціально присвяченим боротьбі з кіберзлочинністю. Конвенція встановлює правові рамки для криміналізації комп'ютерних злочинів, процесуальні інструменти для розслідування кіберзлочинів та механізми міжнародної співпраці у кримінальних справах, пов'язаних з комп'ютерними системами та даними. Україна ратифікувала конвенцію у 2005 році, що стало важливим кроком у гармонізації національного законодавства з європейськими стандартами та забезпечило правову основу для співпраці з іноземними правоохоронними органами у розслідуванні транскордонних кіберзлочинів. Другий додатковий протокол до Будапештської конвенції, відкритий для підписання у 2022 році, посилює механізми транскордонного співробітництва та обміну електронними доказами, відображаючи еволюцію кіберзагроз та необхідність більш

ефективних інструментів міжнародної кооперації [70].

Практичне значення конвенції для України полягає у встановленні спільних стандартів криміналізації та процедур, що дозволяє правоохоронним органам ефективніше співпрацювати з іноземними колегами у розслідуванні злочинів, які часто охоплюють множинні юрисдикції. Водночас О. Корнейко звертає увагу на певні прогалини у застосуванні конвенції в українських реаліях, зокрема недостатню швидкість обміну інформацією між країнами та складність отримання електронних доказів від провайдерів, які знаходяться за кордоном [39]. Ці проблеми особливо гостро постають під час розслідування російських кібератак, коли зловмисники використовують інфраструктуру третіх країн для приховування своєї діяльності.

Паралельно з Будапештською конвенцією з 2019 року розвивається процес розробки нової конвенції ООН про боротьбу з використанням інформаційно-комунікаційних технологій у злочинних цілях, ініційований за ініціативою Росії. Цей процес має на меті створення альтернативного універсального правового інструменту боротьби з кіберзлочинністю. Розбіжності між державами щодо сфери застосування майбутньої конвенції, балансу між правоохоронними повноваженнями та захистом прав людини відображають фундаментальні відмінності у підходах до регулювання кіберпростору. Західні країни та Україна побоюються, що нова конвенція може легітимізувати надмірні державні повноваження щодо контролю Інтернету під приводом боротьби зі злочинністю, що суперечить демократичним цінностям та принципам відкритого Інтернету.

Регіональні правові інструменти відіграють важливу роль у формуванні міжнародно-правових засад кібербезпеки. Європейський Союз розробив найбільш комплексну регіональну систему правового регулювання через директиви про безпеку мережевих та інформаційних систем (NIS Directive 2016, оновлена NIS2 2022), Загальний регламент про захист даних (GDPR 2018), Акт про цифрові послуги та Акт про цифрові ринки. Ці інструменти встановлюють детальні вимоги до кібербезпеки для широкого спектру економічних секторів, створюють механізми координованого реагування на кіберінциденти та забезпечують високі стандарти захисту персональних даних. Для України як

країни-кандидата на вступ до ЄС імплементація цих директив є обов’язковою умовою членства, що вимагає значної трансформації національного законодавства та регуляторної практики.

Т. Ткачук зазначає, що процес адаптації українського законодавства до вимог ЄС у сфері кібербезпеки є одним із найскладніших напрямів євроінтеграції через технічну складність матерії, необхідність створення нових інституційних механізмів та потребу у значних інвестиціях в оновлення критичної інфраструктури [72]. Водночас це створює можливість для модернізації національної системи кібербезпеки відповідно до найвищих європейських стандартів, що підвищить як національну кіберстійкість, так і привабливість України як безпечного простору для цифрового бізнесу та інновацій.

Формування норм відповідальної поведінки держав у кіберпросторі відбувається через діяльність Групи урядових експертів ООН та Робочої групи відкритого складу ООН, які розробляють добровільні норми, правила та принципи кіберповедінки. Консенсусні звіти цих груп підтвердили одинадцять норм, які включають заборону навмисного пошкодження критичної інфраструктури, яка забезпечує надання основних послуг населенню, захист систем реагування на надзвичайні ситуації від кібератак, співпрацю у розслідуванні кіберінцидентів та обмін інформацією про кіберзагрози. Водночас ці норми мають добровільний характер і не передбачають юридично обов’язкових зобов’язань або механізмів забезпечення виконання, що обмежує їх практичну ефективність. На нашу думку, основна цінність цих норм полягає у формуванні спільного розуміння неприйнятної поведінки у кіберпросторі, що може з часом перерости у звичаєве міжнародне право через послідовну практику держав.

Імплементація та дотримання норм відповідальної поведінки у кіберпросторі стикається з викликами, пов’язаними з відсутністю механізмів моніторингу та забезпечення виконання, різним тлумаченням норм державами та складністю верифікації дотримання норм у непрозорому кіберсередовищі. Розвиток заходів зміцнення довіри у кіберпросторі, включаючи обмін національними доктринами кібербезпеки, створення каналів комунікації для

кризових ситуацій та проведення спільних навчань, сприяє зниженню ризиків непорозуміння та ненавмисної ескалації кіберконфліктів. Організація з безпеки та співробітництва в Європі розробила найбільш детальні заходи зміцнення довіри у кіберпросторі серед регіональних організацій. Проте геополітична напруженість часто підриває ефективність цих заходів, особливо у відносинах між державами, які розглядають одна одну як кіберпротивників.

Роль міжнародних організацій у формуванні правових засад кібербезпеки продовжує зростати, при цьому кожна організація має специфічний мандат та підхід. ООН відіграє центральну роль у розробці універсальних норм, НАТО фокусується на колективній кібероборoні та розвитку військових доктрин, Рада Європи через Будапештську конвенцію просуває стандарти боротьби з кіберзлочинністю, а Міжнародний союз електрозв'язку працює над технічними стандартами кібербезпеки. Координація між різними міжнародними організаціями залишається викликом через їхні різні мандати, членство та пріоритети, що може призводити до дублювання зусиль або суперечливих підходів до правового регулювання. Вважаємо, що для України стратегічно важливо активно працювати в усіх релевантних міжнародних платформах: в ООН – для впливу на формування універсальних норм, в НАТО – для розвитку оперативної співпраці у кібероборoні, в Раді Європи – для стандартів правоохоронної діяльності, в структурах ЄС – для адаптації до європейських регуляторних вимог.

Перспективи розвитку міжнародно-правових засад кібербезпеки пов'язані з необхідністю адаптації правового регулювання до нових технологічних викликів, включаючи штучний інтелект, квантові обчислення, Інтернет речей та автономні системи, які створюють принципово нові типи кіберзагроз та правових дилем. Формування правових рамок для регулювання використання штучного інтелекту у кібероперaціях, включаючи питання відповідальності за дії автономних систем, етичні обмеження на використання ШІ для кібератак та механізми забезпечення прозорості алгоритмічних систем безпеки, представляє один із ключових напрямів розвитку міжнародного права кібербезпеки. В. Фурашев підкреслює, що українському законодавцю необхідно вже зараз

закладати правові основи для регулювання цих нових технологій, щоб не опинитися перед необхідністю екстреної адаптації законодавства в майбутньому [74].

Еволюція міжнародно-правових засад кібербезпеки відбувається в умовах геополітичної конкуренції та фундаментальних розбіжностей між державами щодо моделі управління кіберпростором, балансу між безпекою та правами людини, а також ролі недержавних акторів у забезпеченні кібербезпеки. Формування ефективного міжнародно-правового режиму кібербезпеки вимагає подолання цих розбіжностей через діалог, компроміси та поступове наближення позицій. На нашу думку, реалістичною метою для найближчого десятиліття є не створення всеохоплюючої юридично обов'язкової конвенції з кібербезпеки, яка наразі неможлива через геополітичні розбіжності, а поступове зміцнення існуючих норм через їх практичне застосування, розвиток механізмів зміцнення довіри та формування звичаєвого права через послідовну практику держав. Для України це означає необхідність активної участі у всіх релевантних міжнародних процесах, документування російських порушень міжнародного права у кіберпросторі та використання власного досвіду для обґрунтування необхідності посилення міжнародно-правових механізмів відповідальності за кібератаки.

Таким чином, міжнародно-правові засади кібербезпеки перебувають у стані формування та еволюції, поєднуючи адаптацію існуючих норм міжнародного права до цифрового середовища з розробкою нових специфічних правових інструментів. Попри значний прогрес у підтвердженні застосовності міжнародного права до кіберпростору та формуванні добровільних норм поведінки, критичні прогалини залишаються у сферах атрибуції, порогів застосування сили, механізмів забезпечення виконання та балансу між безпекою і правами людини. Розглянуті міжнародно-правові засади створюють нормативну основу для формування та реалізації національних політик кібербезпеки, визначаючи правові межі та можливості для державних дій у кіберпросторі, а також встановлюючи стандарти міжнародної співпраці у протидії кіберзагрозам, що буде детально проаналізовано у наступних розділах дослідження через призму практики провідних держав та міжнародних

організацій.

Висновки до розділу 1

Проведений у першому розділі комплексний аналіз теоретико-методологічних основ дослідження міжнародної кібербезпеки дозволяє сформулювати ряд важливих висновків щодо концептуальної еволюції, теоретичних підходів та міжнародно-правових засад забезпечення безпеки у кіберпросторі.

По-перше, дослідження продемонструвало, що кібербезпека за три десятиліття трансформувалася з вузькотехнічної проблеми захисту комп'ютерних систем у комплексний міждисциплінарний феномен, який охоплює політичні, правові, економічні, соціальні та військові виміри сучасних міжнародних відносин. Еволюція концепту відбувалася через чотири етапи: технократичний підхід 1990-х років, секьюритизація після подій 2001-2007 років, геополітизація у 2010-х роках та сучасне усвідомлення кіберпростору як критичної інфраструктури всього суспільства. Кожен етап відображав зміну розуміння природи кіберзагроз та механізмів протидії їм, демонструючи динамічний характер предмету дослідження.

По-друге, аналіз теоретичних підходів до формування політики у сфері кібербезпеки виявив плюралістичність методологічних перспектив, систематизованих у таблиці 1.1. Порівняльний аналіз реалізму, лібералізму та конструктивізму показав, що для України оптимальним є синтез реалістичного визнання загроз (особливо з боку росії) з ліберальним акцентом на міжнародній співпраці та інтеграції в євроатлантичні структури. Реалізм пояснює необхідність розвитку власних кіберспроможностей та системи стримування, лібералізм обґрунтовує важливість публічно-приватного партнерства та участі у міжнародних режимах, а конструктивізм допомагає зрозуміти процеси формування норм та різні інтерпретації кібербезпеки різними акторами. Додатково, теорії стійкості та управління ризиками надають практичні інструменти для формування політики в умовах обмежених ресурсів та постійних загроз.

По-третє, дослідження міжнародно-правових засад кібербезпеки продемонструвало як досягнення, так і критичні прогалини у формуванні правового режиму кіберпростору. Підтвердження застосовності міжнародного права до кіберпростору Групою урядових експертів ООН у 2013 та 2015 роках створило важливу нормативну основу, проте практична імплементація цього принципу стикається з численними викликами. Ключовими прогалинами залишаються: відсутність універсальних критеріїв визначення порогу застосування сили у кіберпросторі, складність атрибуції кібератак до конкретних держав, відсутність обов'язкових механізмів забезпечення виконання добровільних норм поведінки та різні інтерпретації балансу між безпекою і правами людини. Для України ці прогалини особливо болючі, оскільки попри численні документовані російські кібератаки, міжнародно-правові механізми не забезпечують адекватної відповіді через політичні міркування та юридичні невизначеності.

По-четверте, аналіз показав, що єдиним функціонуючим універсальним інструментом у сфері кіберзлочинності залишається Будапештська конвенція, яку Україна ратифікувала ще у 2005 році. Це забезпечує правову основу для співпраці з європейськими правоохоронними органами, що є критично важливим для розслідування транскордонних злочинів. Водночас паралельний процес розробки конвенції ООН про кіберзлочинність, ініційований Росією, створює ризики формування альтернативного правового режиму з нижчими стандартами захисту прав людини, що вимагає від України активної позиції у захисті європейських цінностей на глобальних платформах.

По-п'яте, встановлено, що для України оптимальною є європейська модель кібербезпеки, яка балансує між захистом суверенітету та збереженням відкритості кіберпростору, між вимогами безпеки та гарантіями прав людини. Імплементація європейських директив NIS2 та GDPR у рамках євроінтеграційного процесу створює можливість для модернізації національної системи кібербезпеки відповідно до найвищих стандартів, що підвищить як національну кіберстійкість, так і міжнародну конкурентоспроможність України. Водночас український досвід протидії масштабним кібератакам в умовах

реального конфлікту є унікальним внеском у глобальне розуміння кібербезпеки та може стати основою для позиціонування України як регіонального центру експертизи.

Таким чином, у першому розділі визначено концептуальну та методологічну основу для подальшого аналізу сучасної міжнародної політики у сфері кібербезпеки. Розуміння еволюції концепту, різноманітності теоретичних підходів та міжнародно-правових рамок є необхідною передумовою для критичного аналізу практики провідних держав, діяльності міжнародних організацій та конкретних кіберінцидентів, які будуть розглянуті у другому розділі дослідження. Особлива увага буде приділена порівнянню американського та китайського підходів як домінуючих парадигм глобального кіберуправління, ролі міжнародних організацій у формуванні архітектури глобальної кібербезпеки та практичним урокам із масштабних кіберінцидентів для вдосконалення міжнародної співпраці у цій сфері.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОЇ МІЖНАРОДНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

2.1. Порівняльна характеристика підходів провідних держав

Сучасна архітектура міжнародної кібербезпеки формується під визначальним впливом двох провідних держав світу – Сполучених Штатів Америки та Китайської Народної Республіки, які представляють кардинально різні філософські, політичні та технологічні підходи до забезпечення безпеки в кіберпросторі. Це протистояння не обмежується суто технічними аспектами кіберзахисту, а охоплює глибинні розбіжності щодо ролі держави в управлінні інформаційними потоками, балансу між індивідуальними правами і колективною безпекою, а також стратегічного використання цифрових технологій для досягнення геополітичних цілей. На нашу думку, аналіз цих двох моделей є ключовим для розуміння глобальної динаміки кібербезпеки, оскільки більшість інших держав змушені або обирати між цими парадигмами, або шукати власні гібридні підходи, що поєднують елементи обох систем відповідно до національних потреб та можливостей.

Американський підхід до кібербезпеки базується на принципах багатостороннього управління кіберпростором, мінімального державного втручання в роботу Інтернету та максимальної свободи інформаційних потоків, що відображає фундаментальні американські цінності індивідуальної свободи, економічного лібералізму та технологічного прогресу. Стратегія національної кібербезпеки США 2023 року визначає п’ять основних стовпів американської політики: захист критичної інфраструктури через партнерство з приватним сектором, руйнування та демантаж загроз через активні кібероперації, формування ринкових сил для стимулювання кіберстійкості, інвестування в стійке майбутнє через технологічні інновації та налагодження міжнародного партнерства для переслідування спільних цілей кібербезпеки. Концептуальною основою американського підходу є визнання того, що більшість критичної цифрової інфраструктури знаходиться у власності та управлінні приватних компаній, що вимагає створення ефективних механізмів публічно-приватного партнерства замість прямого державного контролю над кіберпростором [28].

Інституційна архітектура американської системи кібербезпеки характеризується складною мережею федеральних агенцій, кожне з яких має специфічні повноваження та відповідальність. Агентство кібербезпеки та інфраструктурної безпеки (CISA) відповідає за захист критичної інфраструктури цивільного сектору, Кіберкомандування США (USCYBERCOM) здійснює наступальні та оборонні кібероперацийні в інтересах національної оборони, Національне агентство безпеки (NSA) займається кібершпигунством та технічною розвідкою, Федеральне бюро розслідувань (FBI) розслідує кіберзлочини на території США, а численні галузеві регулятори встановлюють стандарти безпеки для своїх секторів. Координація між цими агенціями здійснюється через Раду національної безпеки та спеціалізовані міжвідомчі комітети, проте децентралізована природа американської системи часто призводить до дублювання функцій та складнощів у забезпеченні єдиної стратегічної лінії. Водночас така децентралізація забезпечує гнучкість та адаптивність системи до швидко змінюваних загроз, дозволяючи різним агенціям спеціалізуватися на специфічних аспектах кіберзахисту [57].

Американська доктрина «постійного залучення» (persistent engagement) передбачає проактивні дії у кіберпросторі для запобігання загрозам до їх реалізації, включаючи збір розвідувальної інформації про потенційних противників, проведення операцій впливу та руйнування ворожої кіберінфраструктури. Ця доктрина відображає американське розуміння кіберпростору як нового домену ведення бойових дій, де традиційні принципи стримування можуть бути неефективними через низький поріг входження для зловмисників, складність атрибуції та асиметричну природу кіберзагроз. Практична реалізація доктрини включає операції «hunt forward», коли американські кіберспеціалісти працюють безпосередньо в мережах країн-партнерів для виявлення та нейтралізації загроз, а також превентивні дії проти кіберзлочинних груп та державних акторів [48]. Вважаємо, що цей підхід є занадто агресивним і створює ризики ескалації, проте для України досвід американської активної оборони може бути корисним у контексті протидії російським кібератакам, особливо в частині превентивного виявлення загроз.

Економічні аспекти американського підходу до кібербезпеки відображають домінування ринкових механізмів та приватних інвестицій у розвиток кіберзахисних технологій, при цьому федеральний уряд виконує переважно координуючу та регулятивну роль. Американський ринок кібербезпеки оцінюється більш ніж у 150 мільярдів доларів щорічно і характеризується високою конкуренцією, швидким впровадженням інновацій та глобальним лідерством у розробці передових технологій кіберзахисту, включаючи штучний інтелект, машинне навчання, квантову криптографію та блокчейн-рішення. Державна підтримка індустрії здійснюється через програми Управління перспективних дослідницьких проектів Міністерства оборони (DARPA), Національного наукового фонду (NSF) та спеціалізованих венчурних фондів, що сприяє швидкому переходу від фундаментальних досліджень до комерційного впровадження інноваційних рішень [40].

Міжнародний вимір американської політики кібербезпеки базується на формуванні широких коаліцій однодумців, просуванні демократичних цінностей у кіберпросторі та протидії авторитарним режимам, які використовують цифрові технології для пригнічення громадянських свобод. Ініціатива «Декларація про майбутнє Інтернету», запущена США у 2022 році та підтримана більш ніж 60 країнами, включаючи Україну, відображає американське бачення відкритого, взаємопов’язаного, безпечного та надійного Інтернету, заснованого на принципах поваги до прав людини та верховенства права. Водночас американська політика передбачає використання економічних санкцій, експортного контролю та інших інструментів примусу проти держав та організацій, які здійснюють зловмисну кібердіяльність, що демонструє готовність використовувати весь спектр національної могутності для забезпечення кібербезпеки [10].

Китайський підхід до кібербезпеки кардинально відрізняється від американської моделі та базується на принципах кіберсуверенітету, централізованого державного контролю над інформаційними потоками та підпорядкування кібербезпеки загальним цілям національного розвитку та забезпечення політичної стабільності. Концепція кіберсуверенітету, яка є

центральним елементом китайської політики, передбачає абсолютне право держави контролювати всі аспекти кіберпростору в межах своїх кордонів, включаючи регулювання інтернет-контенту, управління цифровими платформами, збір та обробку персональних даних громадян та забезпечення відповідності всіх кіберактивностей національним інтересам та цінностям. Стратегія національної кібербезпеки Китаю інтегрована у загальну стратегію національного розвитку та передбачає синхронізацію цілей кібербезпеки з економічною модернізацією, технологічною незалежністю та соціальною стабільністю [6].

Інституційна система китайської кібербезпеки характеризується високим ступенем централізації та ієрархічності, з Центральною групою з питань мережевої безпеки та інформатизації на чолі з Генеральним секретарем Комуністичної партії Китаю як найвищим органом прийняття рішень у сфері кіберполітики. Управління кібербезпекою здійснюється через вертикально інтегровану систему партійно-державних органів, включаючи Міністерство державної безпеки, Міністерство громадської безпеки, Центральний відділ зв’язку ЦК КПК та Народно-визвольну армію Китаю, які тісно координують свою діяльність для забезпечення комплексного контролю над кіберпростором. Така централізована модель забезпечує швидке прийняття та ефективну імплементацію стратегічних рішень, але може обмежувати інноваційність через бюрократичні процедури та політичні міркування [63].

Законодавча база китайської кібербезпеки, яка включає Закон про кібербезпеку (2017), Закон про захист персональних даних (2021) та Закон про безпеку даних (2021), встановлює всеохоплюючі правові рамки для регулювання всіх аспектів кіберпростору. Ці закони передбачають строгі вимоги щодо локалізації даних для критичних галузей, обов’язкове проходження оцінки безпеки для інтернет-продуктів та послуг, а також широкі повноваження державних органів щодо доступу до приватних даних з міркувань національної безпеки. Китайський підхід до регулювання кібербезпеки також включає створення системи соціального кредиту, яка інтегрує кіберповедінку громадян у загальну оцінку їхньої соціальної надійності та може впливати на доступ до

різних державних та комерційних послуг, що демонструє використання цифрових технологій для соціального контролю [24].

Економічна складова китайської політики кібербезпеки тісно пов’язана з стратегією технологічної незалежності та розвитку власних передових технологій у сфері штучного інтелекту, квантових обчислень, 5G-зв’язку та напівпровідників. Китайський уряд здійснює масштабні інвестиції у розвиток національної індустрії кібербезпеки через державні програми, включаючи «Зроблено в Китаї 2025» та стратегію «подвійної циркуляції», які передбачають досягнення технологічного лідерства у критичних сферах цифрової економіки. Особливу увагу китайське керівництво приділяє розвитку власних альтернатив західним технологічним рішенням, що має на меті зменшення залежності від іноземних постачальників та забезпечення повного контролю над критичною цифровою інфраструктурою країни.

Міжнародний аспект китайської політики кібербезпеки базується на просуванні концепції «спільноти єдиної долі в кіберпросторі» та альтернативної моделі управління глобальним Інтернетом, яка передбачає більшу роль суверенних держав у регулюванні кіберпростору та обмеження впливу західних технологічних корпорацій. Китай активно просуває свої цифрові технології та стандарти через ініціативу «Цифровий шовковий шлях», яка є частиною більш широкої програми «Один пояс, один шлях» та передбачає експорт китайських рішень у сфері цифрової інфраструктури, електронної комерції, цифрових платежів та «розумних міст» до країн, що розвиваються. Водночас Китай використовує міжнародні платформи, такі як Всесвітня конференція з Інтернету у Вучжені, для просування альтернативних принципів управління кіберпростором, які підкреслюють суверенітет держав замість універсальних прав людини [36].

Для систематизації та порівняння розглянутих підходів США та КНР нами розроблено таблицю 2.1, яка демонструє ключові відмінності між американською та китайською моделями кібербезпеки за різними параметрами, а також оцінює їх релевантність для української політики в цій сфері.

Таблиця 2.1

Порівняння підходів США та КНР до кібербезпеки

Параметр	США	КНР	Висновок для України
Філософія	Відкритий Інтернет, свобода інформації, мінімальне державне втручання	Кіберсуверенітет, державний контроль, національна безпека понад усе	Баланс: відкритість для інновацій + захист суверенітету від агресії
Роль держави	Мінімальна, регуляторна; держава як координатор та партнер	Централізований контроль; держава як головний актор та регулятор	Середня: активна координація без тотального контролю
Приватний сектор	Автономний, є партнером держави; власник більшості інфраструктури	Під державним контролем; повинен слідувати національним інтересам	Партнерство на рівних; використання потенціалу IT-індустрії
Права людини	Пріоритет (з обмеженнями після 9/11); конституційні гарантії	Підпорядковані безпеці та стабільності; соціальний кредит	Європейська модель балансу: безпека не за рахунок свобод
Технологічна стратегія	Лідерство через інновації, конкуренція, венчурний капітал	Технологічна незалежність, імпортозаміщення, державні інвестиції	Інтеграція в західні ланцюги при розвитку власних спроможностей
Міжнародна позиція	Коаліції однодумців, просування демократичних цінностей	Альтернативна модель, експорт стандартів через «Шовковий шлях»	Євроатлантична інтеграція (НАТО, ЄС)
Регуляторний підхід	Секторальний, ринково-орієнтований, саморегулювання + державний нагляд	Всеохоплюючий, жорсткий, обов’язкова локалізація даних	Імплементація NIS2 та GDPR як стандарт для вступу до ЄС

Джерело: складено автором на основі [28; 6; 35]

Як видно з таблиці 2.1, американська та китайська моделі представляють дві протилежні парадигми організації кібербезпеки, кожна з яких має свою внутрішню логіку та відповідає специфічним політичним системам та культурним традиціям цих країн. Водночас варто зазначити, що бінарне протиставлення «США vs КНР» є певним спрощенням реальної картини. По-перше, навіть у США існує значний державний нагляд, особливо після терористичних атак 11 вересня 2001 року, коли були запроваджені масштабні програми спостереження, такі як PRISM, що викрив Едвард Сноуден у 2013 році.

Це зближує американську практику з китайською, хоча мотивація та правові обмеження залишаються різними. По-друге, Китай демонструє певну гнучкість у кібердипломатії та економічній сфері, особливо через ініціативу «Цифровий шовковий шлях», що не вписується в стереотип жорсткого контролю.

Для України жодна з цих моделей не є повністю прийнятною у чистому вигляді. Американська модель передбачає розвинену технологічну індустрію, потужний приватний сектор та значні фінансові ресурси, яких Україна поки що не має в достатньому обсязі. Китайська модель неприйнятна через свій авторитарний характер, який суперечить демократичним цінностям та європейському вектору розвитку України. На нашу думку, оптимальним для України є європейський підхід, який знаходиться між американською та китайською крайнощами та балансує між захистом суверенітету, стимулюванням інновацій та гарантіями прав людини. Європейські директиви NIS2 та GDPR представляють саме такий збалансований підхід, який Україна має імплементувати як умову вступу до ЄС.

Важливо також враховувати роль інших акторів у глобальній системі кібербезпеки, які пропонують альтернативні моделі та впливають на формування міжнародних стандартів. Європейський Союз позиціонує себе як «регуляторна потуга» (regulatory power), встановлюючи високі стандарти кібербезпеки та захисту даних через директиви та регламенти, які часто стають де-факто глобальними стандартами через «брюссельський ефект» – коли компанії застосовують європейські норми у всьому світі для спрощення операцій. ЄС акцентує увагу на балансі між безпекою, інноваціями та правами людини, що робить цю модель найбільш релевантною для України. Росія розвиває гібридну модель, яка формально визнає приватний сектор, але фактично забезпечує державний контроль та агресивно використовує кібероперацийні як інструмент зовнішньої політики, що робить її небезпечним актором у міжнародному кіберпросторі. Індія прагне зберегти стратегічну автономію, балансуючи між співпрацею з США у технологічній сфері та збереженням власної незалежності в прийнятті рішень щодо кіберпростору.

Технологічні аспекти протистояння між США та Китаєм виходять за межі суто технічних питань та стають частиною більш широкої геостратегічної конкуренції за технологічне лідерство у критичних сферах майбутнього. Американське технологічне лідерство у сфері напівпровідників, програмного забезпечення та інтернет-платформ поступово витісняється китайськими досягненнями у мобільних технологіях, електронній комерції, цифрових платежах та деяких аспектах штучного інтелекту, що створює нову динаміку технологічної біполярності. Торговельна війна між США та Китаєм, яка охоплює критичні технологічні сектори, експортний контроль передових напівпровідників та обмеження доступу до американських технологій для китайських компаній, демонструє, як питання кібербезпеки стають інструментом геополітичної конкуренції. Для України це створює як ризики (необхідність обирати між технологічними екосистемами), так і можливості (використання конкуренції для отримання вигідних умов співпраці).

Вплив американо-китайського протистояння на міжнародну систему проявляється у формуванні двох конкуруючих екосистем цифрових технологій та стандартів, кожна з яких пропонує різні моделі управління кіберпростором. Американська екосистема включає технологічні стандарти кремнієвої долини, правові норми захисту прав людини та принципи ліберального світового порядку. Китайська екосистема базується на державному капіталізмі, технологічному суверенітеті та авторитарному контролі над інформаційними потоками. Це змушує треті країни, включаючи Україну, обирати між різними моделями цифрового розвитку, хоча на практиці більшість країн намагаються зберегти певну гнучкість та не потрапляти в повну залежність від однієї екосистеми. Ця «цифрова холодна війна» створює ризики фрагментації глобального Інтернету та ускладнення міжнародної співпраці у протидії транснаціональним кіберзагрозам.

Практичні результати американського та китайського підходів демонструють, що обидві моделі мають як досягнення, так і проблемні аспекти. Американська модель забезпечує високий рівень технологічних інновацій, конкуренції та адаптивності, але стикається з викликами координації між

численними акторами, захисту критичної інфраструктури приватного сектору та балансування між безпекою і правами людини. Китайська модель демонструє ефективність у швидкій мобілізації ресурсів та досягненні стратегічних цілей, але може обмежувати інноваційність через надмірний контроль, створювати ризики технологічної ізоляції та підривати міжнародну довіру через непрозорість та авторитарні практики. Вважаємо, що український досвід протидії гібридним загрозам демонструє можливість третього шляху – поєднання ефективного кіберзахисту з демократичними цінностями, використання потенціалу ІТ-сектору з державною координацією, інтеграції в західні структури при збереженні власної суб'єктності.

Перспективи еволюції відносин між США та Китаєм у сфері кібербезпеки залежатимуть від здатності обох країн знайти баланс між конкуренцією та співпрацею у вирішенні спільних викликів, таких як кіберзлочинність, тероризм та захист критичної інфраструктури. Можливості для обмеженої співпраці існують у сферах, де інтереси збігаються, включаючи боротьбу з кіберзлочинністю та обмін інформацією про загрози, проте фундаментальні розбіжності у цінностях, геополітичних інтересах та баченні майбутнього світового порядку обмежують потенціал для всебічного партнерства. Для України важливо використовувати це протистояння стратегічно: зміцнювати партнерство з США та ЄС у сфері кібербезпеки, уникати технологічної залежності від будь-якого одного актора та позиціонувати себе як надійного партнера демократичного світу з унікальним досвідом протидії авторитарним кіберзагрозам.

Таким чином, порівняльний аналіз американського та китайського підходів до кібербезпеки розкриває фундаментальні розбіжності у філософії управління кіберпростором, інституційних механізмах забезпечення кіберзахисту та стратегічному використанні цифрових технологій для досягнення національних цілей. Ці розбіжності не обмежуються технічними аспектами, а відображають глибинні суперечності між різними моделями політичного устрою та міжнародної взаємодії, що робить питання кібербезпеки центральним елементом сучасної геополітичної конкуренції. Для України

оптимальним є європейський шлях, який балансує між різними крайнощами та відповідає демократичним цінностям і стратегічному вектору євроатлантичної інтеграції. Розуміння цієї глобальної динаміки є необхідним для аналізу ролі міжнародних організацій у формуванні глобальних норм та механізмів співпраці у сфері кіберзахисту, що буде розглянуто у наступному підрозділі дослідження.

2.2. Роль міжнародних організацій

Сучасна архітектура глобальної кібербезпеки характеризується складною мережею міжнародних організацій, кожна з яких виконує специфічні функції у забезпеченні стабільності та безпеки кіберпростору, при цьому відсутність єдиного глобального регулятора створює як можливості для спеціалізації та інновацій, так і виклики координації та потенційні прогалини у покритті критичних аспектів кібербезпеки. Інституційна фрагментація управління кіберпростором відображає як технічну складність цифрового середовища, так і геополітичні реалії, де різні держави та регіони прагнуть зберегти вплив на формування правил гри у кіберпросторі через участь у різних міжнародних платформах та ініціативах. На нашу думку, ця багатоманітність організацій не є недоліком системи, а радше відображає різні виміри кібербезпеки – від технічного управління інфраструктурою до політичних норм поведінки, від військової кібероборони до правоохоронної співпраці, що вимагає диференційованих інституційних підходів та механізмів координації між ними.

Організація Об’єднаних Націй відіграє центральну роль у формуванні міжнародних норм та принципів кібербезпеки, забезпечуючи універсальну платформу для діалогу між усіма державами-членами незалежно від їхнього рівня технологічного розвитку, політичної системи чи геополітичної орієнтації. Діяльність ООН у сфері кібербезпеки здійснюється через кілька ключових механізмів, серед яких найважливішими є Група урядових експертів з питань інформаційної безпеки та Робоча група відкритого складу з питань безпеки та використання інформаційно-комунікаційних технологій. Консенсусні звіти Групи урядових експертів 2013 та 2015 років встановили фундаментальні

принципи застосовності міжнародного права до кіберпростору, визнання суверенітету держав у кіберсфері та необхідність розробки норм відповідальної поведінки, що створило правову основу для подальшого розвитку міжнародного режиму кібербезпеки [43].

Група урядових експертів традиційно включала представників лише 20-25 держав, обраних за принципом географічного представництва та з урахуванням балансу між різними геополітичними групами, що викликало критику з боку багатьох країн щодо недостатньої інклюзивності процесу. Нездатність Групи досягти консенсусу у 2017 році через розбіжності щодо застосування права на самооборону та міжнародного гуманітарного права до кібероперацій продемонструвала крихкість досягнутих домовленостей та глибину розбіжностей між провідними державами з фундаментальних питань кібербезпеки. Вважаємо, що ця невдача стала важливим уроком про обмеженість ексклюзивних форматів у вирішенні глобальних проблем, що потребують широкої легітимності та участі всіх зацікавлених сторін.

Паралельне створення Робочої групи відкритого складу у 2018 році з ініціативи Росії стало відповіддю на критику ексклюзивності Групи урядових експертів та спробою демократизувати міжнародний діалог через залучення всіх 193 держав-членів ООН до обговорення норм, правил та принципів відповідальної поведінки у кіберпросторі. Робоча група провела безпрецедентні за масштабом консультації з державами, приватним сектором, громадянським суспільством та технічною спільнотою, зібравши сотні письмових внесків та організувавши численні неформальні зустрічі для обговорення широкого спектру питань кібербезпеки. Україна активно брала участь у роботі обох механізмів, використовуючи ці платформи для привернення уваги міжнародної спільноти до російської кіберагресії та просування ідеї посилення міжнародної відповідальності за кібератаки на критичну інфраструктуру [19].

Конвергенція висновків Групи урядових експертів та Робочої групи відкритого складу у їхніх фінальних звітах 2021 року, які підтвердили застосовність міжнародного права, важливість добровільних норм та необхідність заходів зміцнення довіри, продемонструвала наявність базового

консенсусу міжнародної спільноти з фундаментальних принципів кібербезпеки незважаючи на існуючі політичні розбіжності. Створення нової постійної Програми дій ООН з кібербезпеки, яка має розпочати роботу у 2025 році як інституціоналізований механізм для продовження діалогу та імплементації узгоджених норм, відкриває нові можливості для поступового розвитку міжнародного режиму кібербезпеки через регулярні зустрічі, тематичні дискусії та практичну співпрацю між державами. На нашу думку, успіх цієї ініціативи залежатиме від політичної волі держав до компромісів та конкретних дій з імплементації декларованих принципів, а не лише від продовження теоретичних дискусій про норми.

Діяльність ООН у сфері кібербезпеки також включає розробку міжнародної конвенції про боротьбу з використанням інформаційно-комунікаційних технологій у злочинних цілях, переговори щодо якої тривають з 2019 року та відображають складні дискусії між державами щодо балансу між правоохоронними повноваженнями та захистом прав людини. Процес розробки конвенції ускладнюється фундаментальними розбіжностями між різними групами держав щодо сфери застосування майбутнього договору, ступеня деталізації криміналізаційних норм, механізмів міжнародної співпраці та процедурних гарантій захисту прав людини. Водночас спеціалізовані агенції ООН реалізують численні проекти технічної допомоги у сфері кібербезпеки, спрямовані на розвиток спроможностей країн, що розвиваються, у захисті критичної інфраструктури, боротьбі з кіберзлочинністю та формуванні національних стратегій кібербезпеки.

Північноатлантичний альянс представляє найбільш розвинену модель колективної кібероборони, яка еволюціонувала від визнання кіберпростору як операційного домену у 2016 році до інтеграції кіберкомпоненту у всі аспекти планування оборони та військових операцій альянсу. Стратегічна концепція НАТО 2022 року підкреслює критичну важливість кібербезпеки для колективної оборони та визначає кібератаки як потенційний привід для застосування статті 5 Вашингтонського договору про колективну оборону, хоча конкретні пороги та критерії для такого рішення залишаються предметом політичних консультацій

між союзниками. Принцип кіберстійкості НАТО, затверджений у 2016 році, встановлює мінімальні стандарти кібербезпеки для всіх держав-членів та передбачає регулярні оцінки національних спроможностей кіберзахисту, координацію заходів реагування на кіберінциденти та розвиток спільних кіберспроможностей через багатонаціональні проекти [20].

Центр передового досвіду НАТО з питань спільної кіберзахисту у Таллінні відіграє провідну роль у розробці доктринальних основ кібероборони, підготовці військових фахівців та проведенні досліджень з правових аспектів кібервійни, включаючи розробку Таллінського керівництва з міжнародного права, застосовного до кібероперацій них. Кіберкомандування НАТО, створене у 2018 році, координує кіберспроможності альянсу, планує кібероперацій ні на підтримку військових місій та забезпечує захист комунікаційних мереж і систем управління НАТО від кіберзагроз, при цьому воно працює у тісній координації з національними кіберкомандуваннями держав-членів та іншими військовими структурами альянсу. Регулярні кібернавчання НАТО, включаючи масштабні багатонаціональні навчання «Locked Shields» та «Cyber Coalition», демонструють розвиток практичних спроможностей колективної кібероборони та сприяють стандартизації процедур реагування на кіберінциденти серед союзників [60].

Партнерські програми НАТО у сфері кібербезпеки охоплюють країни-кандидати, держави Партнерства заради миру та інші стратегічні партнери, забезпечуючи поширення стандартів та найкращих практик кібербезпеки за межі альянсу. Для України участь у цих програмах є критично важливою для розвитку національних спроможностей кібероборони та підготовки до можливого майбутнього членства в НАТО. Ініціатива «Cyber Defence Pledge», запущена у 2014 році, стимулює збільшення національних інвестицій у кібербезпеку та розвиток інноваційних рішень кіберзахисту через партнерство з приватним сектором та науковими установами. Водночас НАТО активно розвиває співпрацю з Європейським Союзом у сфері кібербезпеки через спільні навчання, обмін інформацією про загрози та координацію заходів реагування на кіберінциденти, що демонструє комплементарність військового та цивільного підходів до забезпечення кібербезпеки у євроатлантичному регіоні.

Міжнародний союз електрозв'язку як спеціалізована агенція ООН відповідальна за координацію глобальних телекомунікаційних послуг та радіочастот відіграє ключову роль у технічних аспектах кібербезпеки та розвитку спроможностей країн, що розвиваються. Глобальна програма кібербезпеки ITU охоплює п'ять стратегічних стовпів: правові заходи, технічні та процедурні заходи, організаційні структури, створення спроможностей та міжнародна співпраця, що забезпечує комплексний підхід до зміцнення глобальної кіберстійкості. Індекс глобальної кібербезпеки ITU, який публікується кожні чотири роки, надає порівняльну оцінку національних спроможностей кібербезпеки та стимулює країни до поліпшення своїх систем кіберзахисту через бенчмаркінг та обмін найкращими практиками, хоча методологія індексу піддається критиці за недостатню увагу до якісних аспектів кібербезпеки та захисту прав людини.

Роль ITU у стандартизації технологій кібербезпеки включає розробку міжнародних стандартів для систем управління інформаційною безпекою, криптографічних протоколів, безпеки мобільних комунікацій та захисту критичної інфраструктури через свої сектори стандартизації. Програми технічної допомоги ITU спрямовані на розвиток національних спроможностей кібербезпеки у країнах, що розвиваються, включаючи створення національних центрів реагування на кіберінциденти, розробку національного законодавства з кібербезпеки, навчання персоналу та впровадження технічних рішень кіберзахисту відповідно до міжнародних стандартів. Вважаємо, що ITU стикається з викликами щодо легітимності та ефективності у сфері кібербезпеки через критику з боку деяких західних країн та громадянського суспільства щодо недостатньої уваги до захисту прав людини та можливого використання технічної допомоги для посилення цифрового нагляду у авторитарних режимах.

Корпорація Інтернет-імен та номерів виконує критично важливу функцію управління системою доменних імен та координації унікальних ідентифікаторів Інтернету, що робить її центральним елементом глобальної інтернет-інфраструктури та важливим актором у забезпеченні кібербезпеки. Передача функцій управління IANA від уряду США до міжнародної спільноти у 2016 році

ознаменувала важливий етап у глобалізації управління Інтернетом та посилила роль ICANN як багатостороннього регулятора критичної інтернет-інфраструктури, хоча ця трансформація також породила нові виклики щодо підзвітності, прозорості та ефективності прийняття рішень в умовах зростаючої геополітичної напруженості. Безпека системи доменних імен є критично важливою для стабільності всього Інтернету, оскільки атаки на DNS можуть призводити до перенаправлення трафіку на шкідливі сайти, блокування доступу до легітимних ресурсів або компрометації конфіденційності користувачів.

Програма захисту DNS-інфраструктури ICANN включає впровадження розширень безпеки системи доменних імен (DNSSEC), моніторинг стабільності та безпеки DNS, координацію реагування на безпекові інциденти та розвиток міжнародного співробітництва з правоохоронними органами у розслідуванні зловживань у сфері доменних імен. Рада консультантів з безпеки та стабільності надає технічні рекомендації щодо загроз безпеці DNS та інтернет-інфраструктури, сприяючи розвитку найкращих практик кібербезпеки серед операторів доменів верхнього рівня та інших учасників екосистеми доменних імен. Водночас ICANN стикається з тиском з боку урядів деяких країн щодо посилення контролю над національними доменами та обмеження доступу до певних інтернет-ресурсів, що створює напруженість між технічною місією організації та політичними вимогами держав щодо кіберсуверенітету [75].

Міжнародна організація кримінальної поліції координує глобальні зусилля правоохоронних органів у боротьбі з кіберзлочинністю, забезпечуючи платформу для обміну інформацією, спільних операцій та розвитку спроможностей національних поліцейських служб у розслідуванні транскордонних кіберзлочинів. Глобальний комплекс цифрових та інноваційних технологій Інтерполу у Сінгапурі служить центром координації міжнародних кібероперацийних, розробки інноваційних інструментів розслідування та навчання поліцейських з усього світу сучасним методам боротьби з кіберзлочинністю, включаючи використання штучного інтелекту, аналізу великих даних та блокчейн-технологій для виявлення та переслідування кіберзлочинців. Операції Інтерполу у боротьбі з кіберзлочинністю демонструють

ефективність міжнародної координації через арешти підозрюваних у множинних країнах та блокування підозрілих банківських рахунків, пов’язаних з онлайн-шахрайством.

Розвиток спроможностей національних правоохоронних органів у сфері кібербезпеки здійснюється через програми навчання Інтерполу, які охоплюють цифрову криміналістику, розслідування кіберзлочинів, міжнародне співробітництво у кримінальних справах та використання сучасних технологій для боротьби зі злочинністю. Глобальна база даних Інтерполу про кіберзлочинність забезпечує централізований обмін інформацією про кіберзагрози, зловмисні програми та підозрюваних осіб, що дозволяє правоохоронним органам різних країн координувати свої дії та відстежувати транскордонну злочинну діяльність у кіберпросторі. Водночас Інтерпол стикається з викликами юрисдикційних обмежень, різних національних законодавств та політичних міркувань, які можуть ускладнювати розслідування кіберзлочинів, особливо у випадках, коли підозрювані перебувають у країнах з обмеженим співробітництвом.

Європейський Союз розробив найбільш комплексну регіональну систему кібербезпеки, яка поєднує наднаціональне регулювання, координацію політики держав-членів та партнерство з приватним сектором для забезпечення кіберстійкості єдиного цифрового ринку. Директива про безпеку мережевих та інформаційних систем NIS2, яка набула чинності у 2023 році, встановлює гармонізовані вимоги до кібербезпеки для критичних та важливих секторів економіки, включаючи енергетику, транспорт, фінансові послуги, охорону здоров’я та цифрову інфраструктуру, що забезпечує мінімальні стандарти кіберзахисту в усіх державах-членах ЄС. Європейське агентство з кібербезпеки (ENISA) координує політику кібербезпеки ЄС, надає технічну підтримку державам-членам, розробляє рекомендації щодо найкращих практик кіберзахисту та здійснює моніторинг загроз кібербезпеці у масштабах всього Союзу.

Механізм координованого реагування на кіберінциденти ЄС забезпечує швидкий обмін інформацією між державами-членами у випадку масштабних

кіберзагроз та координацію спільних заходів реагування, включаючи технічну допомогу, розслідування та відновлення після інцидентів. Європейські центри реагування на кіберінциденти формують інтегровану мережу національних та європейських спроможностей кіберзахисту, яка забезпечує оперативний обмін інформацією про загрози, координацію заходів реагування та взаємну допомогу у випадку кібератак, що перевищують можливості окремих держав-членів. Водночас ЄС розвиває власні наступальні кіберспроможності через створення кіберкомпонентів у структурі Європейської служби зовнішніх справ та розробку режиму кіберсанкцій, який дозволяє застосовувати обмежувальні заходи проти осіб та організацій, відповідальних за кібератаки проти європейських інтересів.

Систематизація ролі різних міжнародних організацій у сфері кібербезпеки представлено на рисунку 2.1, який демонструє багаторівневу архітектуру глобального кіберуправління та показує, як різні організації доповнюють одна одну на різних рівнях та в різних функціональних сферах.

Як видно зі схеми 2.1, архітектура глобального кіберуправління має багаторівневий характер, де кожен рівень виконує специфічні функції та доповнює інші. Глобальний рівень забезпечує легітимність через універсальне представництво та формування базових норм, регіональний рівень деталізує ці норми відповідно до специфічних потреб та можливостей регіонів, технічний рівень забезпечує функціонування критичної інтернет-інфраструктури, а операційний рівень здійснює практичне реагування на кіберінциденти та розслідування злочинів. На нашу думку, ця багаторівнева система є більш ефективною, ніж гіпотетична єдина глобальна організація кібербезпеки, оскільки дозволяє адаптувати підходи до різних аспектів кібербезпеки та враховувати регіональні особливості [21].

Роль регіональних організацій у забезпеченні кібербезпеки демонструє важливість географічної близькості, спільних цінностей та схожих правових систем для ефективної співпраці у протидії кіберзагрозам. Організація з безпеки та співробітництва в Європі розробила комплексні заходи зміцнення довіри у кіберпросторі, які включають обмін національними доктринами кібербезпеки,

створення каналів комунікації для кризових ситуацій, координацію міжнародних навчань та розвиток норм відповідальної поведінки.

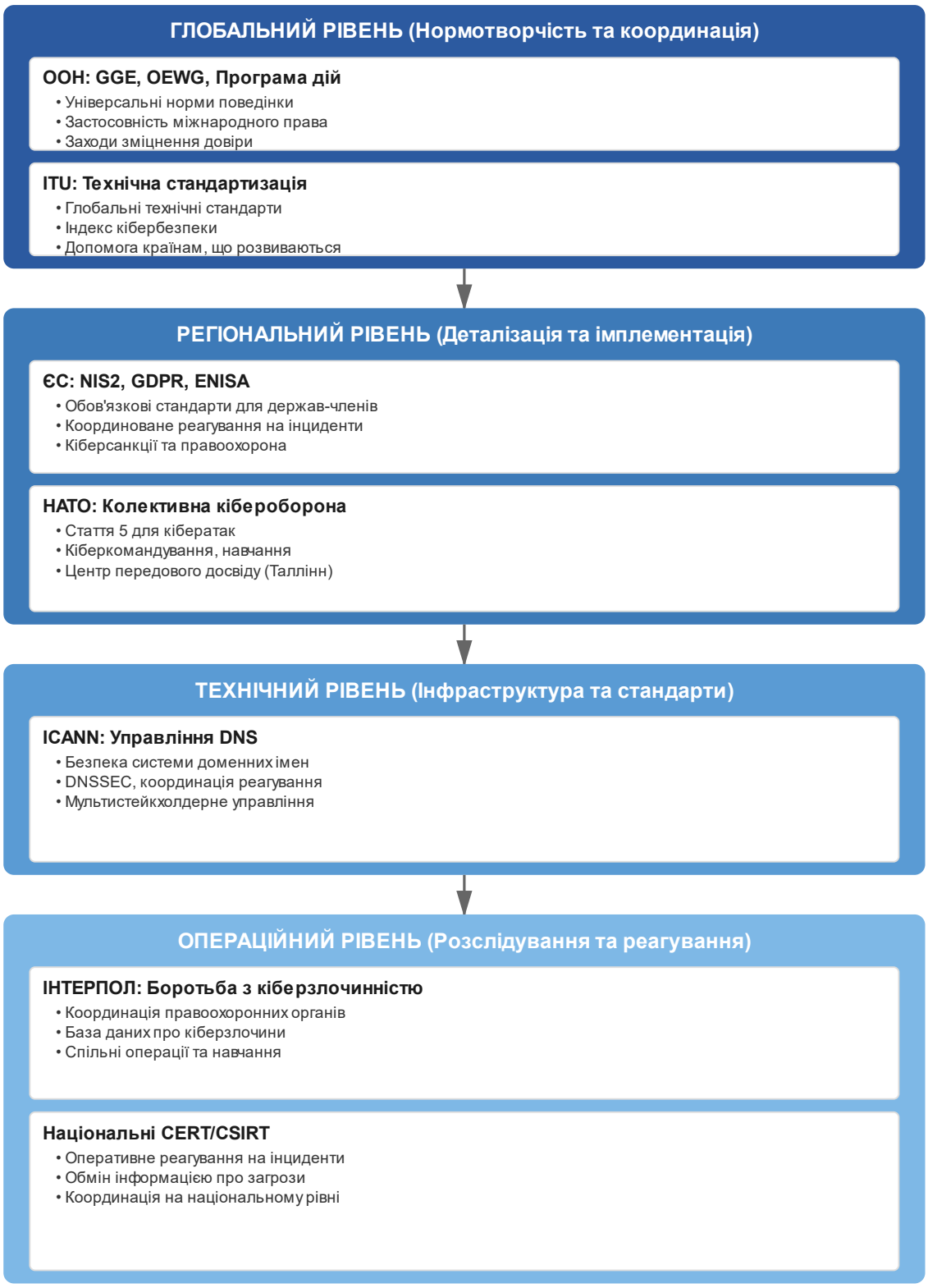

Рис. 2.1. Архітектура глобального кіберуправління

Джерело: розроблено автором

Асоціація держав Південно-Східної Азії прийняла кілька ініціатив у сфері кібербезпеки, включаючи Керівні принципи кібербезпеки АСЕАН, які встановлюють рамки для регіональної співпраці у протидії кіберзагрозам. Африканський Союз розробив континентальну стратегію кібербезпеки та прийняв Конвенцію про кібербезпеку та захист персональних даних, яка створює правові рамки для боротьби з кіберзлочинністю та захисту даних у африканських країнах [13].Виклики координації між різними міжнародними організаціями у сфері кібербезпеки включають дублювання мандатів, конкуренцію за ресурси та увагу держав-членів, різні підходи до регулювання кіберпростору та потенційні протиріччя у рекомендаціях та стандартах. Відсутність чіткого розподілу компетенцій між глобальними, регіональними та спеціалізованими організаціями може призводити до неефективного використання ресурсів, плутанини серед держав-користувачів та прогалин у покритті важливих аспектів кібербезпеки, що вимагає поліпшення координації та співпраці між різними інституційними акторами. Вважаємо, що для України стратегічно важливо активно працювати в усіх релевантних міжнародних платформах: в ООН – для впливу на формування універсальних норм, в НАТО – для розвитку оперативної співпраці у кібероборонні, в Раді Європи – для стандартів правоохоронної діяльності, в структурах ЄС – для адаптації до європейських регуляторних вимог, в Інтерполі – для боротьби з транскордонною кіберзлочинністю [62].

Перспективи розвитку ролі міжнародних організацій у сфері кібербезпеки пов’язані з необхідністю адаптації до нових технологічних викликів, включаючи штучний інтелект, квантові обчислення, Інтернет речей та інші передові технології, які створюють принципово нові типи кіберзагроз та вимагають оновлення існуючих підходів до забезпечення кібербезпеки . Зростаюча складність та взаємопов’язаність глобальної цифрової інфраструктури вимагає посилення координації між технічними та політичними аспектами управління кіберпростором, що може призвести до створення нових міжнародних механізмів або реформування існуючих організацій для кращого відображення сучасних реалій кібербезпеки. Участь недержавних акторів, включаючи технологічні корпорації, громадянське суспільство та академічні установи, у

діяльності міжнародних організацій з кібербезпеки продовжує зростати, що відображає мультистейкхолдерний характер управління кіберпростором та необхідність залучення різних типів експертизи для вирішення комплексних проблем кіберзахисту [17].

Таким чином, аналіз ролі ключових міжнародних організацій у сфері кібербезпеки демонструє складну та багатошарову систему глобального управління кіберпростором, яка характеризується як досягненнями у формуванні норм, стандартів та механізмів співпраці, так і викликами координації, ефективності та адаптації до швидко змінюваних технологічних та геополітичних умов. Різноманітність інституційних підходів та мандатів відображає складність кіберпростору та множинність інтересів різних акторів, при цьому успіх глобальної системи кібербезпеки залежить від здатності цих організацій ефективно співпрацювати, доповнювати один одного та адаптуватися до нових викликів. Для України активна участь у роботі всіх релевантних міжнародних організацій є не лише способом отримання технічної допомоги та доступу до міжнародного досвіду, але й інструментом формування сприятливого міжнародного середовища для протидії російській кіберагресії та просування власних ініціатив щодо посилення міжнародної відповідальності за кібератаки на критичну інфраструктуру. Практична ефективність існуючих механізмів міжнародної координації у сфері кібербезпеки може бути найкраще оцінена через аналіз конкретних кіберінцидентів та міжнародної реакції на них, що буде розглянуто у наступному підрозділі дослідження.

2.3. Кейс-стаді: аналіз кіберінцидентів з міжнародними наслідками

Дослідження конкретних кіберінцидентів з міжнародними наслідками надає унікальну можливість для емпіричного аналізу ефективності існуючих механізмів міжнародної співпраці у сфері кібербезпеки, виявлення прогалин у глобальній системі кіберзахисту та розуміння практичних викликів атрибуції, реагування та відновлення після масштабних кібератак. Методологія кейс-стаді дозволяє проаналізувати складні взаємодії між технічними, політичними,

правовими та економічними аспектами кіберінцидентів, розкрити динаміку міждержавних відносин в умовах кіберкризи та оцінити адекватність теоретичних концепцій кібербезпеки реальним викликам сучасного цифрового світу. На нашу думку, вивчення конкретних випадків є критично важливим для переходу від абстрактних дискусій про норми та принципи до розуміння реальних механізмів, які працюють або не працюють у практиці міжнародної кібербезпеки, особливо в контексті українського досвіду як однієї з найбільш атакованих країн світу.

Кібератака на естонську критичну інфраструктуру у квітні-травні 2007 року стала першим масштабним кіберінцидентом, який продемонстрував вразливість сучасних цифрових суспільств до координованих кібератак та необхідність розробки нових підходів до забезпечення національної безпеки в епоху цифрових технологій. Серія розподілених атак типу відмова в обслуговуванні (DDoS) була спрямована проти урядових веб-сайтів, банківських систем, медіа-ресурсів та телекомунікаційної інфраструктури Естонії, що призвело до суттєвого порушення функціонування критичних сервісів та створило прецедент для розуміння кіберпростору як нового театру конфліктів між державами. Хронологія подій розпочалася після рішення естонського уряду перенести пам’ятник радянським воїнам з центру Таллінна, що спричинило дипломатичну кризу з Росією та масові протести російськомовного населення, при цьому кібератаки розпочалися практично одночасно з вуличними заворушеннями та тривали понад три тижні з різною інтенсивністю [22].

Технічний аналіз естонських кібератак виявив використання ботнетів, що налічували десятки тисяч заражених комп’ютерів по всьому світу, координовані атаки з різних географічних локацій та поступову ескалацію від простих DDoS-атак до більш складних методів. Естонська сторона звинуватила Росію в організації або підтримці кібератак, проте формальних доказів державної причетності надано не було, що ілюструє фундаментальну проблему атрибуції кіберзлочинів та складність застосування традиційних концепцій міжнародної відповідальності до кіберпростору. Російська сторона категорично заперечила будь-яку причетність до кібератак та охарактеризувала їх як спонтанні дії

патріотично налаштованих громадян. Міжнародна реакція на естонські кібератаки стала важливим прецедентом для формування колективних підходів до кіберзахисту, оскільки Естонія звернулася за допомогою до союзників по НАТО та ЄС, які надали технічну експертизу, додаткові ресурси для захисту критичної інфраструктури та політичну підтримку [58].

Водночас інцидент виявив відсутність чітких процедур застосування статті 5 Вашингтонського договору до кібератак, оскільки союзники не розглядали кіберінцидент як збройний напад, що вимагав би колективної відповіді, але надали допомогу у рамках принципів солідарності та взаємопідтримки. Довгострокові наслідки естонських подій включали прискорення розробки національних стратегій кібербезпеки у багатьох країнах, створення Центру передового досвіду НАТО з питань спільної кіберзахисту у Таллінні та початок серйозного обговорення застосовності міжнародного права до кібероперацій в академічних та політичних колах. Вважаємо, що естонський досвід став важливим уроком для України, яка пізніше зіткнулася з набагато більш масштабними та деструктивними російськими кібератаками [12].

Кібератака Stuxnet, виявлена у 2010 році, репрезентує якісно новий тип кіберзброї, спрямованої на фізичне руйнування критичної інфраструктури через кіберзасоби, що ознаменувало перехід від кіберзлочинності та кібершпигунства до повноцінної кібервійни. Складний вірус-черв’як був спеціально розроблений для атаки на промислові системи управління (SCADA) іранських ядерних об’єктів, зокрема підприємства зі збагачення урану в Натанці, та призвів до фізичного пошкодження сотень центрифуг для збагачення урану, що суттєво сповільнило іранську ядерну програму без застосування традиційних військових засобів. Технічна складність Stuxnet, яка включала використання чотирьох раніше невідомих уразливостей нульового дня, складні алгоритми ухилення від антивірусного захисту та специфічні знання промислових процесів збагачення урану, свідчила про державне походження кіберзброї та значні ресурси, інвестовані у її розробку [46].

Атрибуція Stuxnet до спільної операції спецслужб США та Ізраїлю, хоча офіційно ніколи не підтверджувалася, базується на численних розслідуваннях

журналістів, експертному аналізі коду та непрямих свідченнях високопосадовців. Іранська сторона публічно визнала факт кібератаки на свої ядерні об’єкти та звинуватила США та Ізраїль у порушенні міжнародного права, проте уникла масштабної ескалації конфлікту, обмежившись дипломатичними протестами та поступовим нарощуванням власних кіберспроможностей для майбутніх відповідних дій. Непередбачені наслідки Stuxnet включали поширення вірусу за межі цільових іранських об’єктів на тисячі комп’ютерів по всьому світу, що продемонструвало складність контролю кіберзброї та ризики колатерального пошкодження у кіберпросторі.

Stuxnet встановив новий прецедент у міжнародному праві та кіберстратегії, оскільки вперше продемонстрував можливість завдання значної фізичної шкоди критичній інфраструктурі через суто кіберзасоби, що поставило питання про застосовність принципів збройного конфлікту до кібероперацій та необхідність розробки нових норм поведінки у кіберпросторі. Успіх операції стимулював інші держави до розвитку власних наступальних кіберспроможностей та інвестицій у кіберзброю як альтернативу традиційним військовим засобам, що призвело до формування кібернетичної дилеми безпеки. На нашу думку, Stuxnet продемонстрував, що навіть технологічно передові держави можуть стати жертвами кібератак, якщо їхні промислові системи не мають адекватного захисту, що є важливим уроком для України в контексті захисту критичної енергетичної інфраструктури [5].

Кібератаки на українську електроенергетичну систему у грудні 2015 та грудні 2016 років стали першими у світі успішними кібератаками на електромережі, які призвели до масового відключення електроенергії для кількох сотень тисяч споживачів та продемонстрували нові рівні складності та деструктивності кіберзагроз для критичної інфраструктури. Атака 2015 року була спрямована проти трьох енергорозподільних компаній у Західній Україні та включала багаторівневий підхід, який поєднував спир-фішинг для початкового проникнення у корпоративні мережі, латеральний рух по внутрішніх системах для отримання привілеїв, компрометацію промислових систем управління та координовані дії для відключення електричних підстанцій у декількох регіонах

одночасно. Технічний аналіз виявив використання кастомізованого шкідливого програмного забезпечення, включаючи BlackEnergy та KillDisk, які були спеціально адаптовані для атаки на промислові системи [64].

Атака 2016 року на київську енергокомпанію «Укренерго» продемонструвала еволюцію кіберзагроз та використання більш складного шкідливого програмного забезпечення CRASHOVERRIDE (також відомого як Industroyer), яке було спеціально розроблено для атаки на промислові протоколи комунікації та могло потенційно застосовуватися проти енергосистем у будь-якій країні світу. Міжнародна атрибуція цих кібератак до російських військових розвідувальних підрозділів (ГРУ) базувалася на комплексному технічному аналізі, проведеному провідними кібербезпековими компаніями та урядовими агенціями США, Великобританії та інших країн, який виявив зв’язки з попередніми російськими кіберопераціями, використання характерних технік та інфраструктури, а також корреляцію з геополітичними цілями Росії щодо України. Українська сторона офіційно звинуватила Росію в організації кібератак та звернулася за міжнародною підтримкою для посилення кіберзахисту критичної інфраструктури [27].

Міжнародна реакція на українські кіберінциденти включала надання технічної допомоги з боку США, країн ЄС та міжнародних організацій для відновлення постраждалих систем, посилення кіберзахисту енергетичної інфраструктури та розвитку національних спроможностей кіберзахисту. Європейський Союз запустив спеціальну програму підтримки кібербезпеки України, яка включала фінансову допомогу, навчання персоналу, обмін найкращими практиками та розробку спільних стандартів кіберзахисту критичної інфраструктури. Водночас інциденти стимулювали розробку нових міжнародних ініціатив щодо захисту критичної інфраструктури від кібератак. Довгострокові наслідки українських кіберінцидентів включали суттєве посилення міжнародної уваги до захисту енергетичної інфраструктури від кіберзагроз, розробку нових технічних стандартів кібербезпеки для промислових систем управління та прискорення міжнародного співробітництва у сфері обміну інформацією про кіберзагрози.

Кібератака WannaCry у травні 2017 року продемонструвала глобальні масштаби та транскордонний характер сучасних кіберзагроз, оскільки вірус-здирник поширився на сотні тисяч комп'ютерів у більш ніж 150 країнах світу протягом кількох днів та спричинив серйозні порушення у роботі критичних сервісів, включаючи лікарні, транспортні системи, промислові підприємства та урядові установи. Технічною основою WannaCry була уразливість EternalBlue у операційній системі Windows, яка була розроблена Агентством національної безпеки США для розвідувальних цілей, але потрапила у руки кіберзлочинців після витоку інструментів АНБ групою хакерів Shadow Brokers, що ілюструє складні зв'язки між державними кіберпрограмами та злочинною діяльністю у кіберпросторі. Швидкість поширення WannaCry була безпрецедентною через використання червоподібної функції автоматичного сканування та зараження вразливих систем у локальних мережах та через Інтернет [38].

Найбільше постраждалою від WannaCry стала Національна служба охорони здоров'я Великобританії, де понад 200 тисяч комп'ютерів були заражені вірусом, що призвело до скасування тисяч медичних процедур, закриття відділень невідкладної допомоги та серйозних порушень у наданні медичних послуг. Російські організації також постраждали від WannaCry у значних масштабах, що спростовувало первісні припущення про російське походження атаки та підкреслило неконтрольований характер поширення вірусу. Зупинка поширення WannaCry відбулася завдяки випадковому відкриттю механізму зупинки британським дослідником кібербезпеки, що продемонструвало важливість міжнародної співпраці між приватними дослідниками, урядовими агенціями та технологічними компаніями у протидії глобальним кіберзагрозам.

Міжнародна координація реагування на WannaCry включала обмін технічною інформацією між національними центрами реагування на кіберінциденти, спільні зусилля правоохоронних органів у розслідуванні походження вірусу та координацію заходів відновлення між постраждалими організаціями. Європол створив спеціальну робочу групу для координації міжнародного розслідування WannaCry та забезпечив платформу для обміну розвідувальною інформацією між правоохоронними органами різних країн.

Атрибуція WannaCry до північнокорейської хакерської групи Lazarus, здійснена спецслужбами США, Великобританії та інших країн на основі технічного аналізу та розвідувальних даних, стала першим випадком публічної атрибуції масштабної кібератаки до КНДР та призвела до застосування нових санкцій проти північнокорейської кіберпрограми.

Кібератака на Colonial Pipeline у травні 2021 року продемонструвала вразливість критичної енергетичної інфраструктури США до кіберзагроз та економічні наслідки кібератак на системи національного значення. Атака вірусу-здирника DarkSide призвела до вимушеного закриття найбільшого паливного трубопроводу США, який транспортує близько 45% всього палива на східне узбережжя країни, що спричинило дефіцит бензину у кількох штатах, паніку серед споживачів та значні економічні збитки протягом тижневого періоду відновлення операцій. Компанія Colonial Pipeline прийняла рішення про превентивне відключення трубопроводу після виявлення шкідливого програмного забезпечення у своїх комп'ютерних системах, що відображає консервативний підхід до управління ризиками в умовах невизначеності щодо масштабів компрометації критичних систем управління.

Технічний аналіз кібератаки виявив, що зловмисники отримали доступ до мережі Colonial Pipeline через скомпрометовані облікові дані VPN-з'єднання, ймовірно придбані на чорному ринку або отримані через попередні витоки даних, що підкреслює важливість багатофакторної автентифікації та регулярної ротації паролів для захисту віддаленого доступу до критичних систем. Хакерська група DarkSide, яка взяла відповідальність за атаку, функціонувала за моделлю «ransomware-as-a-service», надаючи свої технології іншим кіберзлочинцям в обмін на частку прибутку, що демонструє професіоналізацію та комерціалізацію кіберзлочинності. Компанія Colonial Pipeline врешті-решт заплатила викуп у розмірі приблизно 4,4 мільйона доларів у криптовалюті для отримання ключів дешифрування, хоча пізніше ФБР змогло відновити частину коштів через відстеження блокчейн-транзакцій [76].

Для систематизації та порівняльного аналізу розглянутих кіберінцидентів нами розроблено таблицю 2.2, яка демонструє ключові характеристики кожного випадку, міжнародну реакцію та специфічні уроки для України.

Таблиця 2.2.

Порівняльний аналіз кіберінцидентів з міжнародними наслідками

Інцидент	**Рік**	**Тип загрози**	**Цілі атаки**	**Атрибуція**	**Міжнародна реакція**	**Уроки для України**
Естонія	2007	DDoS-атаки	Уряд, банки, медіа, телеком	Росія (неофіційно, без доказів)	Технічна допомога НАТО/ЄС; політична підтримка	Важливість міжнародної солідарності; необхідність колективних механізмів захисту
Stuxnet	2010	Кіберзброя проти SCADA	Іранські ядерні об’єкти (Натанц)	США + Ізраїль (неофіційно)	Мовчазне визнання; академічні дискусії	Вразливість промислових систем; потреба у сегментації мереж SCADA
Україна (енергетика)	2015-2016	Атаки на критичну інфраструктуру	Енергорозподільні компанії, підстанції	Росія (ГРУ) — офіційна атрибуція США/UK	Технічна допомога ЄС/США; програми розвитку спроможностей	**Критичний** — захист SCADA є національним пріоритетом; сегментація мереж
WannaCry	2017	Ransomware (червоподібний)	Глобальні: лікарні, транспорт, корпорації	КНДР (Lazarus Group)	Координоване реагування через Європол; обмін технічною інформацією	Важливість своєчасного оновлення систем; небезпека витоку державних кіберінструментів
Colonial Pipeline	2021	Ransomware (фінансова мотивація)	Паливний трубопровід США	DarkSide (криміналітет, зв’язки з РФ)	Національна криза; виконавчий указ про кібербезпеку; міжнародне розслідування	Публічно-приватне партнерство; захист ОТ-систем; етика виплати викупів

Джерело: складено автором на основі [1; 4; 7; 10; 13]

Як видно з таблиці 2.2, аналізовані кіберінциденти демонструють еволюцію кіберзагроз від відносно простих DDoS-атак до складних багатоетапних операцій, які поєднують технічну досконаліть з глибоким розумінням цільових систем та стратегічних цілей. Кожен інцидент мав специфічні характеристики та призвів до різних форм міжнародної реакції, проте загальною тенденцією є поступове посилення міжнародної координації у реагуванні на кіберзагрози, хоча значні прогалини залишаються у сферах атрибуції, правової відповідальності та колективного реагування. Порівняльний аналіз показує, що ефективність міжнародної реакції корелює не стільки з масштабом збитків, скільки з геополітичним контекстом: Stuxnet, що створив прецедент кібервійни, не спричинив міжнародного осуду через західне походження атаки, тоді як менш значущі атаки на Естонію отримали політичну підтримку НАТО [9].

Український досвід 2015-2016 років є унікальним: це перші успішні кібератаки на енергосистему з доведеною державною атрибуцією, проте міжнародна реакція обмежилася технічною допомогою без політичних чи економічних санкцій проти Росії, що демонструє недостатність існуючих механізмів відповідальності. Вважаємо, що це є критичною прогалиною міжнародного права кібербезпеки: навіть коли технічно доведено державне походження атаки та її серйозні наслідки для цивільного населення, політичні міркування перешкоджають адекватній відповіді, що фактично заохочує агресорів до продовження кібероперацийних. Для України це означає необхідність продовжувати документування російських кібератак та використовувати всі міжнародні платформи для формування прецедентів відповідальності.

Аналіз показує, що проблема атрибуції залишається однією з найбільших перешкод для ефективного міжнародного реагування, оскільки навіть високоякісний технічний аналіз рідко надає абсолютну впевненість у державній причетності, що залишає простір для правдоподібного заперечення з боку держав-агресорів. Водночас розвиток спроможностей технічної атрибуції та зростання готовності західних держав до публічного оприлюднення результатів

розслідування створюють нові можливості для підвищення відповідальності. Важливим висновком є також те, що роль недержавних акторів, зокрема технологічних компаній та дослідницьких організацій, у реагуванні на кіберінциденти часто виявляється більш ефективною, ніж традиційні урядові механізми завдяки швидкості, гнучкості та технічній експертизі.

Виявлені прогалини у глобальній системі кібербезпеки включають недостатню стандартизацію процедур реагування на кіберінциденти, обмежену ефективність існуючих механізмів атрибуції та відповідальності, а також нерівномірний розвиток кіберспроможностей між різними країнами та регіонами. Складність технічної атрибуції кібератак продовжує створювати виклики для політичного та правового реагування, що залишає простір для заперечень та політичних маніпуляцій. Асиметрія у кіберспроможностях між розвиненими країнами та державами, що розвиваються, створює ризики використання слабких ланок глобальної кіберінфраструктури для атак на більш захищені цілі, що підкреслює необхідність глобального підходу до зміцнення кіберстійкості.

Уроки, отримані з аналізу кіберінцидентів, підкреслюють критичну важливість превентивних заходів, включаючи регулярне оновлення програмного забезпечення, впровадження принципів кіберзахисту ще на етапі проектування систем, навчання персоналу основам кібергігієни та розробку планів безперервності бізнесу для забезпечення швидкого відновлення після кіберінцидентів. Важливість міжнародної координації у реальному часі під час кіберкриз демонструє необхідність створення постійно діючих механізмів комунікації між національними центрами реагування на кіберінциденти, які могли б забезпечувати цілодобовий обмін критичною інформацією та координацію спільних заходів реагування. Роль приватного сектору як власника та оператора більшості критичної цифрової інфраструктури вимагає нових форм публічно-приватного партнерства.

Таким чином, детальний аналіз ключових кіберінцидентів з міжнародними наслідками демонструє складну динаміку взаємодії технічних, політичних, економічних та правових факторів у формуванні сучасного ландшафту

глобальної кібербезпеки, виявляє як досягнення, так і обмеження існуючих механізмів міжнародної співпраці у протидії кіберзагрозам, а також підкреслює необхідність подальшого розвитку комплексних підходів до забезпечення кіберстійкості на національному та міжнародному рівнях. Практичний досвід реагування на масштабні кіберінциденти створює емпіричну основу для вдосконалення теоретичних концепцій кібербезпеки, розробки більш ефективних інструментів кіберзахисту та формування реалістичних стратегій міжнародної співпраці, що враховують як можливості, так і обмеження сучасної системи міжнародних відносин в умовах цифрової трансформації. Для України виклики, виявлені через аналіз цих кейсів, є не абстрактною теорією, а практичною реальністю, що вимагає термінових дій з посилення національної кіберстійкості та активної участі у формуванні міжнародних механізмів відповідальності за кібератаки на критичну інфраструктуру.

Висновки до розділу 2

Комплексний аналіз сучасної міжнародної політики у сфері кібербезпеки, проведений у другому розділі дослідження, дозволяє сформулювати ряд фундаментальних висновків щодо архітектури глобального кіберуправління, динаміки міждержавних відносин у кіберпросторі та ефективності існуючих механізмів міжнародної співпраці у протидії кіберзагрозам.

По-перше, порівняльний аналіз американського та китайського підходів до кібербезпеки, систематизований у таблиці 2.1, виявив фундаментальну поляризацію між двома домінуючими парадигмами — американською моделлю відкритого кіберпростору та китайською концепцією кіберсуверенітету, що створює структурні протиріччя у формуванні універсальних міжнародних норм. Американська парадигма базується на принципах мультистейкхолдерного управління, мінімального державного втручання та домінування ринкових механізмів, тоді як китайська модель передбачає централізований державний контроль, технологічний суверенітет та підпорядкування кіберпростору загальним цілям національного розвитку. Водночас бінарне протиставлення

«США vs КНР» є певним спрощенням, оскільки навіть у США існує значний державний нагляд після подій 11 вересня 2001 року, а Китай демонструє гнучкість у кібердипломатії через «Цифровий шовковий шлях».

Для України жодна з цих моделей не є повністю прийнятною у чистому вигляді. Вважаємо, що оптимальним для України є європейський підхід, який знаходиться між американською та китайською крайнощами та балансує між захистом суверенітету, стимулюванням інновацій та гарантіями прав людини. Європейські директиви NIS2 та GDPR представляють саме такий збалансований підхід, який Україна має імплементувати як умову вступу до ЄС. Український досвід протидії російським кібератакам демонструє можливість третього шляху — поєднання ефективного кіберзахисту з демократичними цінностями, використання потенціалу IT-сектору з державною координацією, інтеграції в західні структури при збереженні власної суб'єктності.

По-друге, дослідження ролі міжнародних організацій у формуванні глобальної архітектури кібербезпеки, візуалізоване через схему 2.1, виявило складну та багатошарову систему інституційного управління, яка характеризується як значними досягненнями у розробці норм та стандартів, так і серйозними викликами координації та ефективності. Організація Об'єднаних Націй зберігає центральну роль у формуванні універсальних принципів кіберповедінки через Групу урядових експертів та Робочу групу відкритого складу, проте повільність консенсусних процедур та геополітичні розбіжності обмежують здатність ООН оперативно реагувати на швидко еволюційні кіберзагрози. НАТО продемонструвало найбільш розвинену модель колективної кібероборони, успішно інтегрувавши кіберкомпонент у всі аспекти планування оборони, що створило важливий прецедент для України як країни-аспіранта на членство в альянсі.

Спеціалізовані технічні організації, такі як ITU та ICANN, відіграють критично важливу роль у забезпеченні стабільності та безпеки глобальної інтернет-інфраструктури, проте їхня діяльність часто стає предметом геополітичної конкуренції. Інтерпол координує глобальні зусилля у боротьбі з кіберзлочинністю, забезпечуючи платформу для обміну інформацією та

спільних операцій. Європейський Союз розробив найбільш комплексну регіональну систему кібербезпеки, яка для України є стратегічним орієнтиром у контексті євроінтеграції. Багаторівнева архітектура глобального кіберуправління, де кожен рівень виконує специфічні функції, є більш ефективною, ніж гіпотетична єдина глобальна організація, оскільки дозволяє адаптувати підходи до різних аспектів кібербезпеки.

По-третє, детальний аналіз конкретних кіберінцидентів з міжнародними наслідками, систематизований у таблиці 2.2, надав емпіричну основу для оцінки практичної ефективності існуючих механізмів міжнародної співпраці та виявив як досягнення, так і серйозні обмеження у глобальній системі кібербезпеки. Еволюція кіберзагроз від естонських DDoS-атак 2007 року до сучасних складних багатоетапних операцій демонструє кардинальну трансформацію природи міжнародної безпеки в цифрову епоху. Проаналізовані інциденти виявили, що ефективність міжнародної реакції корелює не стільки з масштабом збитків, скільки з геополітичним контекстом: Stuxnet не спричинив міжнародного осуду через західне походження атаки, тоді як атаки на Естонію отримали політичну підтримку НАТО.

Український досвід 2015-2016 років є унікальним і особливо важливим: це перші успішні кібератаки на енергосистему з доведеною державною атрибуцією до російських військових розвідувальних підрозділів, проте міжнародна реакція обмежилася технічною допомогою без політичних чи економічних санкцій проти Росії. Це демонструє критичну прогалину міжнародного права кібербезпеки: навіть коли технічно доведено державне походження атаки та її серйозні наслідки для цивільного населення, політичні міркування перешкоджають адекватній відповіді, що фактично заохочує агресорів до продовження кібероперацій них. Для України це означає необхідність продовжувати документування російських кібератак та використовувати всі міжнародні платформи для формування прецедентів відповідальності.

По-четверте, аналіз показав, що проблема атрибуції залишається однією з найбільших перешкод для ефективного міжнародного реагування на кіберзагрози, оскільки навіть високоякісний технічний аналіз рідко надає

абсолютну впевненість у державній причетності, що залишає простір для правдоподібного заперечення з боку держав-агресорів. Водночас розвиток спроможностей технічної атрибуції та зростання готовності західних держав до публічного оприлюднення результатів розслідування кібератак створюють нові можливості для підвищення відповідальності та стримування зловмисної кібердіяльності. Важливим висновком є також те, що роль недержавних акторів, зокрема технологічних компаній та дослідницьких організацій, у реагуванні на кіберінциденти часто виявляється більш ефективною, ніж традиційні урядові механізми завдяки швидкості, гнучкості та технічній експертизі.

По-п’яте, виявлені прогалини у глобальній системі кібербезпеки включають недостатню стандартизацію процедур реагування на кіберінциденти, обмежену ефективність існуючих механізмів відповідальності, нерівномірний розвиток кіберспроможностей між різними країнами та регіонами, а також відсутність ефективних механізмів забезпечення виконання добровільних норм поведінки. Асиметрія у кіберспроможностях між розвиненими країнами та державами, що розвиваються, створює ризики використання слабких ланок глобальної кіберінфраструктури для атак на більш захищені цілі, що підкреслює необхідність глобального підходу до зміцнення кіберстійкості через програми технічної допомоги та розвитку спроможностей.

Загалом проведений аналіз сучасної міжнародної політики у сфері кібербезпеки свідчить про формування складної та суперечливої системи глобального кіберуправління, яка характеризується одночасним існуванням елементів співпраці та конфронтації, інституційними досягненнями та структурними обмеженнями, технологічними інноваціями та політичними перешкодами. Ефективність цієї системи у забезпеченні глобальної кіберстійкості залежатиме від здатності міжнародної спільноти подолати геополітичні розбіжності, адаптувати інституційні механізми до нових технологічних реалій та розробити інноваційні форми співпраці, які враховували б інтереси всіх стейкхолдерів цифрового простору. Для України виклики, виявлені через цей аналіз, є не абстрактною теорією, а практичною реальністю, що вимагає активних дій з посилення національної кіберстійкості, поглиблення

співпраці з євроатлантичними партнерами та використання власного унікального досвіду протидії кіберагресії для формування більш ефективних міжнародних механізмів відповідальності та захисту критичної інфраструктури.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ФОРМУВАННЯ ГЛОБАЛЬНИХ СТАНДАРТІВ У СФЕРІ КІБЕРБЕЗПЕКИ

3.1. Визначення ключових викликів у міжнародному регулюванні кіберпростору

Формування ефективної системи міжнародного регулювання кіберпростору стикається з безпрецедентними викликами, які виходять далеко за межі традиційних проблем міжнародного права та глобального управління. Унікальні технічні характеристики цифрового середовища, швидкість технологічних змін та фундаментальні розбіжності між державами щодо моделі управління кіберпростором створюють складний комплекс перешкод для розробки та імплементації універсальних стандартів кібербезпеки. На нашу думку, аналіз цих викликів є критично важливим не для того, щоб констатувати неможливість глобального регулювання, а навпаки – для визначення реалістичних шляхів поступового формування ефективних механізмів міжнародної співпраці, які враховували б об'єктивні обмеження та використовували б наявні можливості для досягнення практичних результатів.

Першим фундаментальним викликом є проблема визначення самого об'єкта регулювання. Кіберпростір не має чітких географічних меж, які є базовим елементом традиційного міжнародного права, постійно еволюціонує під впливом технологічних інновацій та охоплює складну екосистему технічних систем, інформаційних потоків, соціальних взаємодій та економічних транзакцій. Це ускладнює застосування традиційних концепцій територіальності, юрисдикції та суверенітету, які розроблялися для фізичного світу з його чіткими кордонами та стабільними характеристиками. Транскордонна природа кіберпростору означає, що дії, здійснені в одній юрисдикції, можуть миттєво впливати на системи та користувачів у будь-якій точці світу, створюючи складні юрисдикційні колізії та підриваючи ефективність національного регулювання як основного інструменту правового контролю.

Вважаємо, що ця проблема вимагає переосмислення традиційних правових концепцій. Замість спроб застосувати територіальний принцип до нетериторіального кіберпростору, міжнародне право має розвивати

функціональні підходи, які фокусуються не на тому, де фізично розташовані сервери чи користувачі, а на тому, які ефекти має кібердіяльність та які інтереси вона зачіпає. Український досвід є яскравою ілюстрацією цієї проблеми: російські кібератаки здійснювалися з серверів, розташованих у третіх країнах, використовували інфраструктуру множинних юрисдикцій, але завдавали шкоди конкретно українським об'єктам на території України.

Технологічна складність кіберпростору створює другий вимір регуляторних викликів. Розробка ефективних правових норм вимагає глибокого розуміння технічних аспектів функціонування цифрових систем, яке часто відсутнє у політиків та юристів, відповідальних за формування регуляторної політики. Швидкість технологічних змін перевищує темпи розробки та імплементації правових норм, створюючи постійний розрив між існуючим регулюванням та реальними технологічними можливостями. Будапештська конвенція про кіберзлочинність була прийнята у 2001 році, коли смартфони були рідкістю, соціальні мережі не існували, а хмарні обчислення були футуристичною концепцією. Сьогодні ця конвенція залишається найбільш комплексним міжнародним інструментом, але багато її положень потребують перегляду. Другий додатковий протокол до конвенції, прийнятий у 2022 році, розроблявся майже десять років, за які з'явилися нові технології – штучний інтелект, квантові обчислення, blockchain, – не передбачені навіть у новому протоколі.

На наше переконання, вирішення цієї проблеми лежить у площині розробки більш гнучких та адаптивних регуляторних механізмів. Замість спроб створити детальне всеохоплююче регулювання, яке застаріє ще до його прийняття, міжнародне право має фокусуватися на формуванні загальних принципів та рамок, які можуть бути конкретизовані через технічні стандарти, керівництва та найкращі практики. Це вимагає також більш тісної інтеграції технічних експертів у процеси правотворення та розвитку правової культури, яка визнає обмеженість детального регулювання у швидко змінюваному середовищі.

Третім критичним викликом є фундаментальні розбіжності між провідними державами щодо базових принципів управління кіберпростором. Ці

розбіжності відображають глибинні відмінності у політичних системах, культурних цінностях та стратегічних пріоритетах, що унеможливлює формування універсального консенсусу з ключових питань кібербезпеки. Для західних демократій базовим принципом є свобода інформації та мінімальне державне втручання у функціонування Інтернету. Для Китаю та деяких інших держав кіберпростір є невід'ємною частиною національного суверенітету, де держава має право контролювати інформаційні потоки для забезпечення політичної стабільності та національної безпеки. Ці позиції не є просто різними точками зору – це фундаментально різні розуміння природи кіберпростору та ролі держави в його управлінні.

На нашу думку, це не означає неможливість будь-якої міжнародної співпраці, але вимагає зміни очікувань щодо того, що є реалістично досяжним. Замість пошуків єдиної універсальної моделі управління кіберпростором, міжнародна спільнота має фокусуватися на визначенні мінімального набору спільних норм. Наприклад, заборона кібератак на лікарні під час пандемії або захист систем раннього попередження про ядерні загрози є нормами, які можуть підтримувати держави з різними політичними системами. Водночас для України важливо продовжувати просувати цінності відкритого Інтернету та захисту прав людини, навіть якщо ці принципи не стануть універсально визнаними.

Четвертий виклик пов'язаний з проблемою атрибуції кібероперацій, яка залишається однією з найбільших технічних та правових перешкод для ефективного міжнародного регулювання. Анонімність та можливість маскування справжнього джерела кібератак ускладнюють встановлення відповідальності. Навіть найсучасніші методи технічної атрибуції рідко надають абсолютно переконливі докази державної причетності, залишаючи простір для правдоподібного заперечення. Український досвід є яскравою ілюстрацією цієї проблеми: міжнародні експерти документально довели російське походження численних кібератак на українську енергетичну інфраструктуру, включаючи атрибуцію до конкретних підрозділів ГРУ, проте це не призвело до застосування адекватних міжнародно-правових санкцій проти Росії.

Вважаємо, що проблема атрибуції має дві складові: технічну та політичну. Технічна складова поступово вирішується через розвиток спроможностей аналізу та міжнародної співпраці. Політична складова є більш складною, оскільки навіть за наявності переконливих доказів держави можуть уникати публічної атрибуції через небажання ескалації конфлікту або економічні інтереси. Для подолання цієї проблеми необхідно розвивати механізми колективної атрибуції, коли не одна держава, а група країн або міжнародна організація офіційно визнає джерело атаки, що підвищує політичну ціну заперечення.

П'ятий виклик полягає у мультистейкхолдерному характері кіберпростору, де критичну роль відіграють не лише держави, але й приватні корпорації, громадянське суспільство, технічна спільнота та індивідуальні користувачі. Приватний сектор володіє та управляє більшістю критичної цифрової інфраструктури, розробляє ключові технології та стандарти, надає основні цифрові послуги та часто має більші технічні експертизи та ресурси для забезпечення кібербезпеки, ніж державні установи. Технологічні гіганти контролюють глобальні платформи та інфраструктуру, від яких залежать мільярди людей та тисячі урядів. Вони приймають рішення про стандарти безпеки, політики приватності, модерацію контенту, які мають глобальні наслідки, часто без значного державного нагляду.

На наше переконання, мультистейкхолдерний характер кіберпростору є не недоліком, який треба виправити через посилення державного контролю, а об'єктивною реальністю, яку треба визнати та інтегрувати у механізми глобального управління. Для України це означає необхідність розвитку ефективного публічно-приватного партнерства, де держава виконує координуючу та регуляторну роль, але активно залучає потужний вітчизняний IT-сектор до забезпечення національної кібербезпеки.

Шостий виклик пов'язаний з асиметрією кіберспроможностей між різними державами та регіонами. Країни з різним рівнем технологічного розвитку мають різні пріоритети у сфері кіберзахисту. Глобальний індекс кібербезпеки ITU за 2020 рік показує значні розбіжності між країнами: якщо лідери рейтингу мають

комплексні національні стратегії та розвинене законодавство, то країни у нижній частині рейтингу часто не мають навіть базових елементів національної системи кібербезпеки [1]. Ця нерівність має практичні наслідки для глобальної безпеки: кіберзлочинці використовують юрисдикції зі слабкими правоохоронними спроможностями як безпечні гавані, а глобальні кіберепідемії поширюються швидше через незахищені системи.

На нашу думку, подолання цифрового розриву має розглядатися не як акт благодійності, а як інвестиція у глобальну безпеку. Програми розвитку спроможностей та технічна допомога є прагматичною необхідністю для забезпечення безпеки всього кіберпростору. Для України участь у програмах міжнародної допомоги є критично важливою для підтримання високого рівня кіберстійкості, водночас український досвід може бути цінним для інших країн.

Сьомий виклик стосується балансування між вимогами кібербезпеки та захистом фундаментальних прав і свобод людини. Заходи кібербезпеки часто передбачають розширення державного нагляду, обмеження анонімності та контроль над інформаційними потоками. Різні держави мають кардинально відмінні підходи до цього балансу: від ліберальних демократій, які намагаються мінімізувати обмеження прав людини, до авторитарних режимів, які використовують аргументи кібербезпеки для виправдання тотального контролю. Ця дилема має конкретні практичні прояви: чи має держава право вимагати створювати «задні двері» у шифруванні для доступу правоохоронців? Які межі збору метаданих? Чи виправдане блокування вебсайтів для протидії дезінформації?

Вважаємо, що для України як демократичної держави критично важливо дотримуватися високих стандартів захисту прав людини навіть в умовах серйозних кіберзагроз. Це стратегічне питання ідентичності: на відміну від авторитарних сусідів, Україна має демонструвати, що ефективна кібербезпека можлива без жертвування демократичними цінностями. Практика останніх років показує, що це можливо: попри масштабні російські кібератаки, Україна зберігає відкритий Інтернет та дозволяє громадянам користуватися шифрованими комунікаціями.

Восьмий виклик пов'язаний з відсутністю ефективних механізмів забезпечення виконання міжнародних норм та стандартів кібербезпеки. Традиційні інструменти міжнародного права часто виявляються неефективними для реагування на порушення у кіберпросторі через складність атрибуції та швидкість розвитку подій. Коли у 2017 році вірус NotPetya, атрибутований до Росії, завдав глобальних збитків на понад 10 мільярдів доларів, міжнародна спільнота обмежилася дипломатичними заявами та символічними санкціями. Не було механізму компенсації збитків, міжнародного суду чи навіть консенсусу щодо порушення міжнародного права. Ця безкарність фактично заохочує держави-агресори до продовження кібероперацій.

На наше переконання, створення ефективних механізмів забезпечення виконання є найскладнішим викликом, оскільки вимагає обмеження державного суверенітету на користь колективних інтересів. Можливими кроками могли б стати: створення спеціалізованого арбітражу з кіберспорів, розробка режиму колективних санкцій, формування механізмів компенсації збитків та посилення політичної ціни порушень через систематичну публічну атрибуцію.

Дев'ятий виклик пов'язаний з проблемою подвійного використання кібертехнологій. Ті самі інструменти можуть використовуватися як для легітимних цілей кібербезпеки, так і для зловмисних кібератак. Історія Stuxnet та витоку інструментів АНБ групою Shadow Brokers ілюструє цю проблему: державні інструменти потрапили у руки зловмисників та були використані для глобальної епідемії WannaCry. Водночас будь-які спроби обмежити розробку кіберінструментів стикаються з проблемою визначення меж між оборонними та наступальними технологіями.

Десятий виклик стосується проблеми стійкості та адаптивності регуляторних систем. У швидко змінюваному середовищі регуляторні рамки повинні бути одночасно достатньо стабільними для забезпечення передбачуваності та достатньо гнучкими для адаптації до нових технологій. Вважаємо, що ідеальна система має поєднувати стабільні принципи вищого рівня з адаптивними механізмами імплементації нижчого рівня. Фундаментальні

принципи мають бути закріплені на рівні міжнародних договорів, тоді як технічні стандарти мають бути достатньо гнучкими для швидкого оновлення.

Таким чином, міжнародне регулювання кіберпростору стикається з комплексом взаємопов'язаних викликів, які випливають з фундаментальних характеристик кіберпростору як транскордонного, швидко еволюційного, технічно складного та політично суперечливого домену. Визнання глибини цих викликів є необхідною передумовою для розробки реалістичних стратегій міжнародної співпраці. Для України розуміння цих викликів критично важливе для формування власної позиції у міжнародних процесах регулювання кіберпростору та ефективного використання ресурсів для максимізації кіберстійкості в умовах гібридної війни. Водночас ці виклики не означають неможливість міжнародного регулювання – вони лише вказують на необхідність реалістичних очікувань та інноваційних підходів.

3.2. Шляхи формування глобальних норм та стандартів кібербезпеки

Визначивши у попередньому підрозділі комплекс викликів, які ускладнюють міжнародне регулювання кіберпростору, переходимо до аналізу практичних механізмів їх подолання. Ключове запитання полягає не в тому, чи можливе формування глобальних норм за наявності таких серйозних перешкод, а в тому, які реалістичні шляхи ведуть до поступового створення ефективного режиму кібербезпеки. Досвід останніх двох десятиліть переконує, що навіть без всеохоплюючих міжнародних договорів відбувається органічний розвиток практики держав, технічних специфікацій та неформальних правил поведінки. Вважаємо за доцільне відмовитися від ілюзій щодо швидкого створення універсальної системи регулювання на зразок традиційних режимів роззброєння. Натомість продуктивнішим є фокус на конкретних кроках, здатних дати результат навіть в умовах геополітичного протистояння.

Теоретично процес формування норм доцільно розглядати крізь призму еволюційного інституціоналізму. Глобальний порядок виникає не через централізоване проектування, а через інтеракцію численних акторів, які

керуються власними інтересами, проте поступово формують спільні патерни через навчання та адаптацію. Така перспектива має важливі практичні наслідки: замість пошуку єдиного оптимального рішення треба заохочувати різноманітність експериментів на різних рівнях, налагоджувати обмін досвідом між юрисдикціями, забезпечувати гнучкість для швидкої адаптації. Еволюційний підхід передбачає, що ефективні практики поступово витісняють неефективні через механізми добровільного наслідування успішних моделей, а не через примус.

Аналіз існуючих механізмів дозволяє виокремити три базові моделі нормотворення. Традиційна міждержавна дипломатія через ООН забезпечує легітимність завдяки універсальності, однак страждає від консенсусних процедур та можливості блокування прогресу окремими державами. Регіональна інтеграція через ЄС чи НАТО дозволяє досягати амбітніших результатів через спільність цінностей, проте обмежена географічно й ризикує фрагментацією глобального простору. Мультистейкхолдерне управління залучає технічну експертизу приватного сектору, але викликає питання демократичної легітимності. На наше переконання, оптимальним є гібридний підхід, який комбінує ці моделі залежно від специфіки питання: базові принципи потребують санкції ООН, деталізовані стандарти ефективніші регіонально, технічні протоколи краще розробляти професійним спільнотам.

Розпочнемо з процесів під егідою Організації Об'єднаних Націй. Група урядових експертів та Робоча група відкритого складу сформували консенсус щодо застосовності міжнародного права до кіберпростору й одинадцяти добровільних норм поведінки. Принциповим є питання трансформації цих декларацій у практичні інструменти. Український кейс ілюструє проблему: Росія формально підтримала норми про незавдання шкоди критичній інфраструктурі, водночас систематично атакувала українську енергетику. Розрив між риторикою та практикою є фундаментальним викликом для міжнародного права.

Наступний етап має фокусуватися на операціоналізації існуючих норм. Абстрактні принципи потребують конкретизації через індикатори дотримання, процедури звітування, механізми верифікації. Створення реєстру національних

законів щодо кібербезпеки, регулярні національні звіти про імплементацію, процедури peer review для оцінки зусиль окремих країн – ці механізми не матимуть юридичної обов'язковості, проте створюватимуть репутаційні стимули через підвищення прозорості. Програма дій ООН, що стартує у 2025 році, надає інституційну рамку для такої операціоналізації через забезпечення постійного діалогу замість епізодичних зустрічей експертних груп.

Критично важливим доповненням є механізми зміцнення довіри між державами. Заходи confidence-building у кіберпросторі включають обмін інформацією про національні доктрини та організаційні структури, створення каналів екстреної комунікації, попередні консультації перед впровадженням політик із транскордонними ефектами, добровільне повідомлення про значні інциденти. ОБСЄ розробила найдетальнішу систему таких заходів, хоча після 2014 року їх ефективність знизилася через погіршення загальної атмосфери довіри. Це підкреслює обмеженість CBMs: вони корисні для зменшення ризиків непорозумінь між державами, що прагнують співіснування, але безсилі перед цілеспрямованою агресією. Для України підтримка таких механізмів з європейськими партнерами залишається важливою для координації спільних дій, тоді як ілюзії щодо довіри з Росією були б небезпечними до припинення агресії.

Паралельно розвивається регіональна стандартизація, де Європейський Союз демонструє найуспішнішу модель. Директива NIS2 встановлює обов'язкові вимоги для держав-членів із наднаціональним механізмом нагляду через Європейську Комісію. Декілька характеристик пояснюють ефективність цієї моделі. По-перше, обов'язковість на противагу добровільним нормам ООН. По-друге, наднаціональний контроль, незалежний від політичної кон'юнктури окремих столиць. По-третє, інтеграція кібербезпеки у логіку єдиного цифрового ринку, що створює економічні стимули через доступ до спільного ринку. По-четверте, принцип мінімальної гармонізації дозволяє національні варіації за умови дотримання базових стандартів.

Розглядаючи європейську модель з української перспективи, бачимо амбівалентність. Імплементація NIS2 вимагає не просто технічної транспозиції законодавства, а системної трансформації управління кібербезпекою: нові

інституції, регуляторні спроможності, інвестиції в інфраструктуру, культурні зміни у бізнесі. Масштаб завдання є колосальним, особливо за війни та дефіциту ресурсів. Водночас саме ця необхідність адаптації створює можливість стрибка у розвитку через чітку дорожню карту, міжнародну підтримку та політичний мандат для складних реформ. Український парадокс полягає в тому, що країна, яка зазнає найінтенсивніших кібератак у світі, має шанс побудувати найсучаснішу систему кіберзахисту саме через поєднання практичного досвіду протидії загрозам із доступом до передових європейських стандартів.

Третій вимір формування стандартів реалізується через технічні організації та професійні спільноти. Їхня логіка функціонування радикально відрізняється від державоцентричних підходів. Стандарти ISO 27000 не мають юридичної сили, проте широко застосовуються добровільно, оскільки сертифікація створює конкурентні переваги: довіру клієнтів, спрощення відносин з регуляторами, зниження страхових премій. Ця модель функціонує через ринкові механізми, а не владні повноваження. Деполітизація технічної стандартизації є її перевагою – експерти досягають консенсусу з питань, непереборних для політиків через ідеологічні розбіжності.

Однак ідеалізувати цей процес не варто. Технічні стандарти ніколи не є цілком нейтральними – вони відображають інтереси тих, хто їх розробляє. Зростаюча конкуренція між США та Китаєм за вплив у міжнародних організаціях стандартизації демонструє геополітизацію навіть суто технічних питань. Китай активно просуває своїх експертів у керівні органи ITU, ISO та інших організацій, намагаючись закласти у глобальні стандарти принципи, сумісні з моделлю кіберсуверенітету. Західні держави протидіють цьому через власні делегації експертів та стратегічне використання процедурних механізмів. Результатом може стати фрагментація технічних стандартів на конкуруючі екосистеми, що підриватиме глобальну інтероперабельність.

Принципово важливим механізмом є публічно-приватне партнерство. Оскільки приватний сектор володіє більшістю критичної інфраструктури, його залучення є не опцією, а необхідністю. Традиційна модель командно-контрольного регулювання неефективна у швидкозмінному технологічному

середовищі. Потрібен перехід до моделі співтворення, де держава та бізнес спільно розробляють рішення. Cybersecurity Tech Accord, підписаний понад сотнею компаній, демонструє потенціал корпоративної саморегуляції: добровільні зобов'язання захищати користувачів і не брати участі у наступальних операціях проти цивільних цілей.

Ефективне партнерство вимагає від держави готовності ділитися розвідувальною інформацією про загрози, забезпечувати правову визначеність для компаній, що співпрацюють добросовісно, створювати економічні стимули через податкові пільги чи державні закупівлі. Від бізнесу – готовності інвестувати у безпеку понад мінімальні регуляторні вимоги, обмінюватися інформацією про інциденти та вразливості, брати соціальну відповідальність за вплив своїх продуктів на суспільну безпеку. Український досвід IT Army під час повномасштабного вторгнення демонструє унікальний потенціал добровільної мобілізації технологічної спільноти. Інституціоналізація цього досвіду через формалізовані механізми обміну інформацією, спільні навчання та координоване реагування могла б стати моделлю для інших країн.

Четвертий шлях пролягає через розвиток спроможностей країн з обмеженими ресурсами. Подолання цифрового розриву є не благодійністю, а прагматичною інвестицією у глобальну безпеку. Глобальний індекс кібербезпеки ITU фіксує драматичні розбіжності: лідери мають комплексні стратегії та інституції, тоді як країни в нижній частині рейтингу часто не мають навіть базових елементів кіберзахисту [1]. Ця асиметрія має конкретні наслідки: кіберзлочинці експлуатують слабкі юрисдикції як безпечні гавані, глобальні епідемії поширюються через незахищені системи у бідніших регіонах.

Програми технічної допомоги мають фокусуватися не лише на постачанні обладнання, а передусім на передачі знань та навичок. Адаптація рішень до місцевого контексту критична для успіху – стандартні пакети часто не працюють через невідповідність інституційним реаліям країн-реципієнтів. Забезпечення ownership через активну участь національних стейкхолдерів у плануванні програм підвищує їх ефективність. Україна може відігравати подвійну роль: як реципієнт допомоги для зміцнення власної кіберстійкості та як донор

практичного досвіду протидії реальним загрозам. Створення регіонального центру передового досвіду на базі українських інституцій стало б платформою обміну уроками з країнами Східної Європи, Кавказу та Центральної Азії.

П'ятий напрямок реалізується через судову практику та правоохоронну співпраці. Національні суди формують юриспруденцію застосування традиційних правових концепцій до цифрового середовища. Європейський суд з прав людини встановив стандарти балансу між масовим кібернаглядом та правом на приватність у кількох важливих рішеннях. Міжнародні трибунали починають розглядати питання кваліфікації кібероперацій за міжнародним гуманітарним правом. Ця казуїстична еволюція через судові рішення поступово конкретизує абстрактні норми.

Будапештська конвенція залишається центральним інструментом правоохоронної кооперації попри свій вік. Другий додатковий протокол, прийнятий у 2022 році, посилює механізми транскордонного обміну електронними доказами – критичний елемент для ефективного розслідування. Розширення географічного охоплення конвенції через приєднання нових учасників поступово створює глобальну мережу держав із сумісними правовими рамками для боротьби з кіберзлочинністю. Інтерпол координує міжнародні операції через Глобальний комплекс у Сінгапурі, забезпечуючи платформу обміну розвідувальними даними та спільних арештів.

Шостим механізмом є розвиток відповідальності та стримування. Публічна атрибуція кібератак підвищує репутаційні ризики для порушників навіть без формальних санкцій. США, ЄС та їхні союзники дедалі частіше оприлюднюють детальні звіти про походження масштабних атак із технічними доказами та атрибуцією до конкретних підрозділів іноземних спецслужб. Економічні санкції проти осіб та організацій, причетних до кіберзлочинності, стають стандартним інструментом. Дипломатична ізоляція через обмеження співпраці у технологічних сферах створює додаткові стимули. Однак ефективність цих заходів обмежена складністю досягнення міжнародного консенсусу.

Створення формалізованих механізмів колективної відповідальності посилило б стримуючий ефект. Спеціалізований арбітраж з кіберспорів при ООН

або іншій організації міг би розглядати претензії держав щодо порушень узгоджених норм. Режим автоматичних санкцій проти систематичних порушників, подібний до механізмів у сфері нерозповсюдження ядерної зброї, підвищив би ціну безкарності. Фонд компенсації збитків від кібератак, фінансований міжнародною спільнотою, забезпечив би відновлення постраждалих країн та створив би економічні стимули для превенції. Для України просування таких ініціатив є стратегічним пріоритетом – документування російських атак може стати основою майбутніх претензій про компенсацію та формування прецедентів відповідальності.

Сьомий напрямок реалізується через освіту, дослідження та формування глобальної експертної спільноти. Академічні установи та аналітичні центри генерують знання, що інформують політичні рішення. Таллінське керівництво з міжнародного права, хоч і не має офіційного статусу, стало найвпливовішим довідником для розуміння застосування МГП до кібероперацій них. Міжнародні конференції та публікації створюють простір для обміну ідеями та формування епістемічних спільнот, що поділяють спільне розуміння проблем попри національні кордони.

Інвестиції України у розвиток національної експертизи через підтримку академічних програм, дослідницьких центрів та участь у міжнародних ініціативах є критичними для інтелектуального лідерства. Український досвід протидії кіберагресії має документуватися, аналізуватися та систематизуватися у формі case studies, академічних публікацій, навчальних матеріалів. Це не лише збереже унікальні знання для майбутніх поколінь, а й забезпечить Україні роль інтелектуального центру глобальних дискусій про кібербезпеку.

Нарешті, восьмий шлях стосується адаптивного регулювання нових технологій. Штучний інтелект, квантові обчислення, Інтернет речей створюють принципово нові загрози та можливості. Регуляторні пісочниці дозволяють експериментувати з інноваційними рішеннями у контрольованому середовищі перед масовим впровадженням. Для зрілих технологій потрібні конкретні стандарти, базовані на оцінці ризиків. Проактивний підхід до регулювання має

формувати траєкторію розвитку технологій у напрямку безпеки за дизайном замість реактивного виправлення проблем.

Міжнародна координація у регулюванні нових технологій критична для уникнення фрагментації ринку. Різні юрисдикції обиратимуть різні підходи відповідно до пріоритетів, що вимагає механізмів взаємного визнання еквівалентності стандартів та інтероперабельності систем. Для України раннє прийняття прогресивних стандартів може створити репутацію надійного партнера для міжнародного технологічного бізнесу.

Таким чином, формування глобальних норм кібербезпеки відбувається не через один магістральний шлях, а через комбінацію множинних механізмів на різних рівнях. Кожен має свої сильні сторони та обмеження. Синергія між ними створює складну екосистему нормотворення, де універсальні принципи ООН забезпечують легітимність, регіональні стандарти – деталізацію, технічні специфікації – практичну реалізацію, публічно-приватне партнерство – залучення ресурсів, програми розвитку – глобальну стійкість, судова практика – конкретизацію, механізми відповідальності – стимули дотримання, освіта – інтелектуальну основу, адаптивне регулювання – готовність до майбутнього. Для України розуміння цієї багатовимірності критичне для стратегічного позиціонування у глобальних процесах та максимізації впливу через активну участь у всіх релевантних ініціативах.

3.3. Пропозиції щодо формування ефективної моделі глобального управління кібербезпекою: досвід для України

Формування ефективної моделі глобального управління кібербезпекою вимагає системного переосмислення існуючих підходів та розробки інноваційних механізмів, які враховували б технологічні реалії цифрової епохи, геополітичні трансформації сучасного світового порядку та специфічні потреби різних категорій стейкхолдерів, при цьому особливої уваги заслуговує досвід України, яка стала полігоном для випробування найсучасніших кіберзагроз та водночас демонструє унікальні можливості для розвитку національної

кіберстійкості в умовах постійного зовнішнього тиску. Пропозиції щодо вдосконалення глобальної архітектури кібербезпеки повинні базуватися на реалістичній оцінці існуючих викликів та обмежень, врахуванні накопиченого досвіду успішних та невдалих ініціатив, а також інтеграції інноваційних підходів, які дозволили б подолати структурні протиріччя між різними моделями управління кіберпростором.

Першим елементом запропонованої моделі має стати створення багаторівневої системи глобального кіберуправління, яка поєднувала б універсальні принципи та норми на глобальному рівні з гнучкими механізмами імплементації на регіональному та національному рівнях, дозволяючи державам адаптувати міжнародні стандарти до своїх специфічних умов без підриву загальної ефективності системи. Така архітектура передбачала б формування базового набору фундаментальних принципів кібербезпеки, обов'язкових для всіх учасників міжнародної системи, включаючи заборону кібератак на критичну інфраструктуру, яка забезпечує життєдіяльність цивільного населення, захист систем реагування на надзвичайні ситуації, відповідальність держав за кібердіяльність з їхньої території та обов'язок співпраці у розслідуванні транскордонних кіберзлочинів.

Водночас модель повинна передбачати достатню гнучкість для врахування різних підходів до балансування між безпекою та правами людини, ролі держави в управлінні кіберпростором та механізмів співпраці з приватним сектором, визнаючи легітимність різних моделей за умови дотримання базових принципів. Регіональні організації, такі як ЄС, АСЕАН, Африканський союз або Організація американських держав, могли б розробляти більш детальні стандарти та механізми співпраці, адаптовані до специфічних потреб та можливостей своїх регіонів, створюючи проміжний рівень між глобальними нормами та національним регулюванням, що забезпечило б поступову конвергенцію різних підходів через практичну співпрацю та обмін досвідом.

Другим ключовим компонентом ефективної моделі має стати інституціоналізація мультистейкхолдерного підходу через створення Глобальної ради з кібербезпеки, яка об'єднувала б представників держав, міжнародних

організацій, приватного сектору, громадянського суспільства, технічної спільноти та академічних кіл у постійно діючому форматі для координації зусиль, обміну інформацією та розробки спільних рішень. На відміну від існуючих платформ, які часто мають консультативний характер або обмежене представництво, Глобальна рада повинна мати чіткі повноваження щодо розробки технічних стандартів, координації реагування на масштабні кіберінциденти, управління програмами розвитку спроможностей та моніторингу виконання міжнародних зобов'язань у сфері кібербезпеки.

Структура Глобальної ради могла б включати тематичні комітети з питань критичної інфраструктури, боротьби з кіберзлочинністю, захисту прав людини в цифровому середовищі, розвитку спроможностей та технологічних інновацій, кожен з яких об'єднував би відповідних експертів та стейкхолдерів для розробки спеціалізованих рішень. Фінансування діяльності Ради могло б здійснюватися через комбінацію державних внесків, пропорційних до розміру національних економік та рівня цифровізації, приватних інвестицій від технологічних компаній, які отримували б вигоди від стабільного та безпечного кіберпростору, та міжнародних грантів для підтримки участі країн, що розвиваються, забезпечуючи інклюзивність процесу без надмірного навантаження на окремих учасників.

Третім елементом моделі повинна стати система градуйованих механізмів реагування на порушення норм кібербезпеки, яка включала б дипломатичні, економічні та технічні інструменти впливу, адаптовані до специфіки кіберпростору та пропорційні до тяжкості порушень. Замість традиційної бінарної системи «порушення - санкції», яка часто виявляється неефективною через складність атрибуції та політичні міркування, градуйована система передбачала б спектр можливих відповідей від публічної атрибуції та дипломатичного осуду до обмеження доступу до міжнародних механізмів кіберспівпраці, технічної ізоляції зловмисних акторів та координованих економічних санкцій у найбільш серйозних випадках.

Важливим інноваційним елементом могло б стати створення механізму «кіберкарантину» для держав або недержавних акторів, які систематично

порушують норми кібербезпеки або дозволяють використовувати свою територію для кібератак, що передбачало б тимчасове обмеження їхньої можливості підключатися до глобальних цифрових сервісів та інфраструктури до усунення джерел загрози. Технічна реалізація такого механізму вимагала б співпраці провідних інтернет-провайдерів, операторів магістральних мереж та платформ хмарних сервісів, що підкреслює критичну важливість залучення приватного сектору до системи глобального кіберуправління не лише як об’єкта регулювання, але й як активного партнера у забезпеченні кіберстійкості.

Четвертим компонентом ефективної моделі має стати комплексна система розвитку глобальних кіберспроможностей, яка виходила б за межі традиційних програм технічної допомоги та передбачала б системну трансформацію національних екосистем кібербезпеки у країнах з обмеженими ресурсами через довгострокові партнерства, трансфер технологій та розвиток локальної експертизи. Глобальний фонд кібербезпеки з початковим капіталом у 10 мільярдів доларів, сформований через внески розвинених країн, технологічних корпорацій та міжнародних фінансових інституцій, міг би фінансувати програми навчання кіберспеціалістів, створення національних центрів реагування на кіберінциденти, розробку національного законодавства та стратегій кібербезпеки, а також впровадження базових технічних заходів захисту критичної інфраструктури.

П’ятим елементом моделі повинна стати система превентивної кібердипломатії, спрямована на запобігання ескалації кіберконфліктів та мінімізацію ризиків ненавмисних кіберінцидентів через механізми раннього попередження, канали кризової комунікації та процедури деескалації. Створення регіональних центрів кіберстабільності, які функціонували б як нейтральні платформи для обміну інформацією про кіберзагрози, координації спільного реагування на інциденти та медіації кіберспорів між державами, могло б суттєво знизити ризики переростання технічних інцидентів у політичні кризи або військові конфлікти, особливо в регіонах з високим рівнем геополітичної напруженості.

Механізми «кібергарячих ліній» між національними центрами кібербезпеки, аналогічні до ядерних гарячих ліній часів холодної війни, забезпечили б можливість швидкої комунікації між потенційними противниками для з'ясування природи кіберінцидентів, запобігання помилковій атрибуції та координації зусиль з мінімізації колатеральної шкоди від кібератак. Регулярні спільні кібернавчання між державами, включаючи потенційних геополітичних суперників, могли б сприяти формуванню спільного розуміння червоних ліній у кіберпросторі, розвитку довіри між кіберспільнотами різних країн та виробленню спільних процедур реагування на транскордонні кіберінциденти.

Шостим компонентом запропонованої моделі має стати система технологічної нейтральності та відкритих стандартів, яка забезпечувала б інтероперабельність різних національних та корпоративних систем кібербезпеки, запобігала б технологічній фрагментації кіберпростору та стимулювала б інновації через конкуренцію різних рішень на основі об'єктивних критеріїв ефективності. Глобальний реєстр сертифікованих рішень кібербезпеки, які пройшли незалежну верифікацію на відповідність міжнародним стандартам безпеки та приватності, допоміг би організаціям та державам обирати надійні технології без необхідності проведення власної складної експертизи, особливо важливо для країн з обмеженими технічними ресурсами.

Для України, яка перебуває на передовій кіберпротистояння та водночас прагне інтегруватися у європейську та євроатлантичну спільноту, запропонована модель відкриває унікальні можливості для трансформації викликів у конкурентні переваги через розвиток національної індустрії кібербезпеки, експорт набутого досвіду протидії складним кіберзагрозам та позиціонування як регіонального центру кіберстійкості. Український досвід успішної протидії масштабним кібератакам у реальних бойових умовах, розвитку державно-приватного партнерства у сфері кіберзахисту та мобілізації громадянського суспільства для протидії інформаційним загрозам створює унікальну експертизу, яка може бути цінною для інших країн, що стикаються з подібними викликами.

Як зазначає провідний експерт з кібербезпеки Джеймс Льюїс: «Україна перетворилася з об'єкта кібератак на лабораторію кіберстійкості, де

випробовуються та вдосконалюються найсучасніші підходи до захисту критичної інфраструктури, протидії гібридним загрозам та забезпечення функціонування державних сервісів в умовах постійного кібертиску». Цей досвід може стати основою для української ініціативи щодо створення Міжнародного центру протидії гібридним загрозам у Києві, який став би платформою для обміну досвідом, навчання спеціалістів та розробки інноваційних рішень для країн, що стикаються з подібними викликами.

Інтеграція України у запропоновану модель глобального управління кібербезпекою могла б відбуватися через активну участь у регіональних європейських механізмах з поступовим розширенням до глобального рівня, використання статусу країни-кандидата на членство в ЄС для гармонізації національного законодавства з європейськими стандартами кібербезпеки та розвиток стратегічного партнерства з НАТО у сфері кібероборони. Створення в Україні регіонального хабу для розвитку кіберспроможностей країн Східної Європи та Чорноморського регіону, підтриманого міжнародними донорами та технологічними компаніями, могло б перетворити країну з реципієнта допомоги на активного контрибутора до регіональної кіберстійкості.

Сьомим елементом моделі повинна стати система адаптивного регулювання, яка дозволяла б швидко реагувати на появу нових технологій та загроз без необхідності тривалих переговорів та ратифікації нових міжнародних угод через механізми «регуляторних пісочниць», експериментальних проектів та ітеративного вдосконалення норм на основі практичного досвіду. Щорічний глобальний огляд кіберзагроз та ефективності існуючих механізмів протидії, підготовлений незалежною групою експертів на основі даних від усіх стейкхолдерів, забезпечував би емпіричну основу для коригування стратегій та пріоритетів, дозволяючи системі еволюціонувати відповідно до змін технологічного та геополітичного ландшафту.

Восьмим компонентом має стати механізм інклюзивної участі малих та середніх держав у формуванні глобальних норм кібербезпеки через створення коаліцій однодумців, які могли б колективно просувати свої інтереси та пропозиції на міжнародних форумах, компенсуючи обмежені індивідуальні

ресурси через синергію зусиль. Для України участь у таких коаліціях, наприклад у форматі «Люблінського трикутника» з Польщею та Литвою або ширшої ініціативи країн «Тримор'я», могла б посилити її вплив на формування європейських та глобальних стандартів кібербезпеки, забезпечити доступ до передових технологій та експертизи, а також створити додаткові механізми колективного захисту від кіберзагроз.

Важливим аспектом запропонованої моделі є визнання кібербезпеки як глобального суспільного блага, яке вимагає колективних інвестицій та зусиль для забезпечення, подібно до боротьби зі зміною клімату або пандеміями, що могло б стати основою для нової парадигми міжнародної співпраці, заснованої на спільній відповідальності за стабільність кіберпростору. Це передбачало б перехід від вузького розуміння кібербезпеки як питання національної безпеки окремих держав до визнання взаємозалежності всіх учасників цифрової екосистеми та необхідності спільних дій для забезпечення її стійкості, що могло б створити нові стимули для співпраці навіть між геополітичними суперниками.

Дев'ятим елементом моделі повинна стати система економічних стимулів для дотримання стандартів кібербезпеки, яка включала б преференційний доступ до міжнародних ринків для компаній та країн, що демонструють високий рівень кіберзахисту, страхові механізми для компенсації збитків від кібератак за умови дотримання базових стандартів безпеки, та фінансову підтримку для впровадження передових технологій кіберзахисту. Глобальний індекс кіберстійкості, який враховував би не лише технічні аспекти кіберзахисту, але й правові, організаційні та людські фактори, міг би стати основою для диференційованого підходу до надання міжнародної допомоги, інвестицій та торговельних преференцій, створюючи позитивні стимули для покращення національних систем кібербезпеки.

Десятим, завершальним елементом запропонованої моделі має стати механізм постійного навчання та адаптації через систематичний аналіз кіберінцидентів, обмін найкращими практиками та колективне вироблення уроків з успіхів та невдач у забезпеченні кібербезпеки на різних рівнях. Глобальна база знань з кібербезпеки, доступна для всіх стейкхолдерів з

диференційованим рівнем доступу залежно від чутливості інформації, забезпечила б накопичення та систематизацію колективного досвіду, дозволяючи новим учасникам швидко підвищувати свій рівень компетенції та уникати повторення помилок інших.

Успішна імплементація запропонованої моделі вимагатиме поетапного підходу, починаючи з пілотних проектів у окремих регіонах або секторах з поступовим розширенням до глобального масштабу, що дозволило б протестувати різні елементи системи, виявити та усунути недоліки, а також сформувати критичну масу підтримки серед ключових стейкхолдерів. Для України оптимальною стратегією було б зосередитися на тих елементах моделі, де країна має найбільші конкурентні переваги або критичні потреби, зокрема на розвитку регіональних механізмів кіберстійкості, експорті набутого досвіду протидії гібридним загрозам та залученні міжнародної підтримки для відновлення та модернізації критичної інфраструктури з урахуванням найвищих стандартів кібербезпеки.

Реалізація запропонованої моделі могла б трансформувати глобальну систему кібербезпеки з фрагментованої сукупності національних та регіональних ініціатив у інтегровану екосистему, здатну ефективно протидіяти сучасним та майбутнім кіберзагрозам, забезпечувати стабільність критичної інфраструктури та захищати права і свободи людей у цифровому просторі. Хоча повна імплементація всіх елементів моделі може зайняти десятиліття та вимагатиме подолання значних політичних, технічних та економічних перешкод, поступовий прогрес у окремих напрямках може принести відчутні результати вже у короткостроковій перспективі, створюючи позитивну динаміку для подальшого розвитку системи.

За оцінкою Всесвітнього економічного форуму: «Майбутнє глобальної кібербезпеки залежить від здатності міжнародної спільноти подолати традиційні обмеження державоцентричного підходу та створити інноваційні механізми управління, які поєднували б ефективність централізованої координації з гнучкістю децентралізованої імплементації, забезпечуючи баланс між безпекою та свободою, суверенітетом та взаємозалежністю, інноваціями та стабільністю».

Запропонована модель намагається досягти цього балансу через комплексний підхід, який враховує різноманітність інтересів та можливостей учасників глобального кіберпростору, створюючи рамки для конструктивної співпраці навіть в умовах геополітичної напруженості та технологічної невизначеності.

Таким чином, формування ефективної моделі глобального управління кібербезпекою вимагає системного підходу, який поєднував би інституційні інновації, технологічну нейтральність, економічні стимули та механізми інклюзивної участі всіх стейкхолдерів у забезпеченні стабільності та безпеки кіберпростору. Для України інтеграція у цю систему відкриває можливості трансформації з об’єкта кіберагресії на активного контрибутора до глобальної кіберстійкості, використовуючи унікальний досвід протидії гібридним загрозам для розвитку національної індустрії кібербезпеки та зміцнення міжнародних позицій країни у цифровому світі, що створює передумови для формулювання комплексних висновків щодо перспектив розвитку глобальних стандартів кібербезпеки та їх значення для забезпечення стабільності міжнародної системи в епоху цифрових трансформацій.

Висновки до розділу 3

Проведений у третьому розділі комплексний аналіз перспектив формування глобальних стандартів у сфері кібербезпеки дозволяє сформулювати ряд фундаментальних висновків щодо сучасного стану, потенціалу та майбутнього розвитку міжнародної системи управління кіберпростором. Дослідження виявило, що процес формування ефективних глобальних стандартів кібербезпеки стикається з безпрецедентними викликами, які виходять далеко за межі традиційних проблем міжнародного співробітництва та вимагають принципово нових підходів до управління транснаціональними технологічними системами в умовах геополітичної фрагментації та швидкої технологічної еволюції.

Ідентифікація ключових викликів у міжнародному регулюванні кіберпростору продемонструвала системну невідповідність між глобальною

природою цифрових технологій та фрагментованістю політичних, правових та економічних систем, які намагаються їх регулювати. Транскордонність кіберпростору, швидкість технологічних змін, проблема атрибуції кібероперацій, мультистейкхолдерний характер цифрової екосистеми та фундаментальні розбіжності між державами щодо моделі управління кіберпростором створюють структурні перешкоди для формування універсальних стандартів, прийнятних для всіх учасників міжнародної системи. Особливо критичними виявилися протиріччя між вимогами кібербезпеки та захистом прав людини, між економічною ефективністю та безпековими стандартами, між технологічними інноваціями та регуляторною стабільністю, що вимагає постійного пошуку складних компромісів та балансів.

Аналіз потенціалу існуючих глобальних ініціатив виявив парадоксальну ситуацію, коли множинність платформ, процесів та механізмів співпраці створює ілюзію активної діяльності, але не призводить до формування цілісної та ефективної системи глобального кіберуправління. Діяльність Групи урядових експертів ООН та Робочої групи відкритого складу продемонструвала можливість досягнення базового консенсусу щодо застосовності міжнародного права до кіберпростору та важливості норм відповідальної поведінки, проте відсутність механізмів імплементації та забезпечення виконання цих норм суттєво обмежує їх практичний вплив. Мультистейкхолдерні ініціативи, такі як Паризький заклик, показали потенціал мобілізації широких коаліцій державних та недержавних акторів, але їх добровільний характер та відсутність участі ключових кібердержав знижують ефективність таких механізмів у вирішенні найгостріших проблем кібербезпеки.

Розроблені пропозиції щодо формування ефективної моделі глобального управління кібербезпекою базуються на визнанні необхідності системної трансформації існуючих підходів через створення багаторівневої архітектури, яка поєднувала б універсальні принципи з гнучкими механізмами регіональної та національної імплементації. Запропонована модель передбачає інституціоналізацію мультистейкхолдерного підходу через створення Глобальної ради з кібербезпеки, систему градуйованих механізмів реагування на

порушення норм, комплексні програми розвитку спроможностей, механізми превентивної кібердипломатії та економічні стимули для дотримання стандартів безпеки. Критично важливим є визнання кібербезпеки як глобального суспільного блага, що вимагає колективних зусиль та інвестицій всіх учасників цифрової екосистеми незалежно від їхніх політичних розбіжностей чи економічної конкуренції.

Особливе значення має аналіз можливостей України в контексті формування глобальних стандартів кібербезпеки, який показав, що країна володіє унікальним досвідом протидії складним кіберзагрозам в умовах реального конфлікту, що може стати цінним внеском у розвиток міжнародної кіберстійкості. Трансформація України з об'єкта кіберагресії на активного контрибутора до глобальної кібербезпеки можлива через розвиток національної індустрії кіберзахисту, експорт набутого досвіду, створення регіональних механізмів співпраці та активну участь у формуванні міжнародних норм та стандартів. Запропоноване створення в Україні Міжнародного центру протидії гібридним загрозам могло б перетворити країну на регіональний хаб кіберстійкості та платформу для обміну досвідом між країнами, що стикаються з подібними викликами.

Загальний висновок полягає в тому, що формування ефективних глобальних стандартів кібербезпеки є не просто технічним або правовим завданням, а фундаментальним викликом для всієї системи міжнародних відносин, який вимагає переосмислення традиційних концепцій суверенітету, безпеки та глобального управління в контексті цифрової трансформації. Успіх у цій сфері залежатиме від здатності міжнародної спільноти подолати геополітичні розбіжності, створити інноваційні механізми співпраці між державними та недержавними акторами, забезпечити баланс між різними цінностями та інтересами, а також адаптувати регуляторні механізми до швидкості технологічних змін. Хоча повна реалізація запропонованої моделі може зайняти десятиліття, поступовий прогрес у окремих напрямках вже сьогодні може створити позитивну динаміку для формування більш безпечного, стабільного та

інклюзивного глобального кіберпростору, що є критично важливим для забезпечення сталого розвитку цифрової цивілізації у XXI столітті.

ВИСНОВКИ

Проведене дослідження міжнародної політики у сфері кібербезпеки дозволяє сформулювати комплекс узагальнень теоретичного та практичного характеру, які розкривають складну динаміку формування глобального режиму регулювання кіберпростору, виявляють ключові виклики та можливості міжнародної співпраці у протидії кіберзагрозам, а також визначають стратегічні перспективи для України в контексті інтеграції у євроатлантичні структури безпеки.

Еволюція концепту кібербезпеки за останні три десятиліття відображає поступову трансформацію від вузькотехнічної проблеми захисту комп'ютерних систем до комплексного міждисциплінарного феномену, який охоплює політичні, правові, економічні, соціальні та військові виміри сучасних міжнародних відносин. Дослідження виявило чотири основні етапи цієї еволюції: технократичний підхід 1990-х років, коли кібербезпека розглядалася переважно як технічна проблема захисту мереж; секьюритизація після серії масштабних кіберінцидентів 2001-2007 років, що призвела до визнання кіберзагроз питанням національної безпеки; геополітизація у 2010-х роках, коли кіберпростір став ареною міждержавного протистояння та інструментом досягнення стратегічних цілей; сучасне усвідомлення кіберпростору як критичної інфраструктури всього суспільства, від якої залежить функціонування держави, економіки та базових соціальних сервісів.

Теоретичний аналіз підходів до формування політики кібербезпеки продемонстрував, що жодна окрема парадигма міжнародних відносин не здатна повністю пояснити складну реальність глобального кіберпростору. Реалізм адекватно описує міждержавну конкуренцію та роль сили у кіберпросторі, проте недооцінює можливості співпраці та значення недержавних акторів. Лібералізм правильно акцентує важливість міжнародних інституцій та економічної взаємозалежності, але занадто оптимістично оцінює перспективи досягнення консенсусу між державами з фундаментально різними ціннісними системами. Конструктивізм пояснює процеси формування норм та ідентичностей у кіберпросторі, водночас недостатньо враховує матеріальні обмеження та владні

відносини. На наше переконання, оптимальним для розуміння міжнародної політики кібербезпеки є синтетичний підхід, який поєднує реалістичне визнання конфліктності міжнародної системи з ліберальним акцентом на можливості інституційної кооперації та конструктивістським розумінням значення ідей та норм.

Аналіз міжнародно-правових засад кібербезпеки виявив як досягнення, так і критичні прогалини у формуванні правового режиму кіберпростору. Підтвердження застосовності міжнародного права до кіберпростору Групою урядових експертів ООН створило важливу нормативну основу, проте практична імплементація цього принципу стикається з численними викликами. Ключовими прогалинами залишаються відсутність універсальних критеріїв визначення порогу застосування сили у кіберпросторі, складність атрибуції кібероперацій них до конкретних держав, відсутність обов'язкових механізмів забезпечення виконання добровільних норм поведінки та різні інтерпретації балансу між безпекою і правами людини. Будапештська конвенція про кіберзлочинність залишається єдиним функціонуючим універсальним інструментом правоохоронної співпраці, проте її географічне охоплення та предметна сфера потребують розширення для адекватної відповіді на сучасні виклики.

Порівняльний аналіз американського та китайського підходів до кібербезпеки розкрив фундаментальну поляризацію між двома домінуючими парадигмами організації кіберпростору. Американська модель базується на принципах мультистейкхолдерного управління, мінімального державного втручання, домінування ринкових механізмів та пріоритету індивідуальних прав над колективною безпекою. Китайська парадигма передбачає централізований державний контроль, технологічний суверенітет, підпорядкування кіберпростору загальним цілям національного розвитку та пріоритет політичної стабільності над особистими свободами. Це протистояння виходить за межі суто технічних питань, відображаючи глибинні розбіжності у політичних системах та баченні майбутнього світового порядку. Для України жодна з цих моделей не є повністю прийнятною у чистому вигляді — оптимальним є європейський підхід,

який балансує між різними крайнощами та відповідає демократичним цінностям і стратегічному вектору євроатлантичної інтеграції.

Дослідження ролі міжнародних організацій виявило складну багаторівневу архітектуру глобального управління кіберпростором, де різні інституції виконують комплементарні функції. Організація Об'єднаних Націй забезпечує універсальну платформу для формування базових принципів через інклюзивний діалог. НАТО розвиває найбільш передову модель колективної кібероборони через інтеграцію кіберкомпоненту у всі аспекти планування оборони. Європейський Союз створив найкомплекснішу регіональну систему регулювання через обов'язкові директиви та наднаціональний нагляд. Спеціалізовані технічні організації, такі як ITU та ICANN, забезпечують стабільність критичної інтернет-інфраструктури. Інтерпол координує глобальні правоохоронні зусилля у боротьбі з кіберзлочинністю. Ця інституційна різноманітність є не недоліком через відсутність єдиного центру управління, а перевагою через можливість адаптувати підходи до специфіки різних аспектів кібербезпеки.

Аналіз конкретних кіберінцидентів з міжнародними наслідками надав емпіричну основу для оцінки практичної ефективності існуючих механізмів міжнародної співпраці. Естонські події 2007 року стали першим масштабним кіберінцидентом, який продемонстрував вразливість цифрових суспільств та необхідність колективної відповіді. Stuxnet 2010 року встановив прецедент використання кіберзброї для фізичного руйнування критичної інфраструктури. Атаки на українську енергетику 2015-2016 років були першими успішними кібератаками на електромережі з доведеною державною атрибуцією. WannaCry 2017 року продемонстрував глобальні масштаби та транскордонний характер сучасних загроз. Colonial Pipeline 2021 року виявив вразливість критичної інфраструктури розвинених країн до ransomware. Порівняльний аналіз цих інцидентів показав, що ефективність міжнародної реакції корелює не стільки з масштабом збитків, скільки з геополітичним контекстом, що підкреслює політизацію питань кібербезпеки.

Український досвід є особливо показовим: попри документовану атрибуцію численних російських кібератак до конкретних підрозділів військової розвідки та серйозні наслідки для цивільного населення, міжнародна реакція обмежилася технічною допомогою без адекватних політичних чи економічних санкцій проти агресора. Це демонструє критичну прогалину міжнародного права кібербезпеки: навіть за наявності переконливих доказів державної відповідальності політичні міркування перешкоджають рішучій відповіді, що фактично заохочує продовження кібероперацій. Для України це означає необхідність продовжувати систематичне документування російських атак та використовувати всі міжнародні платформи для формування прецедентів відповідальності.

Визначення ключових викликів у міжнародному регулюванні кіберпростору виявило, що перешкоди мають не тимчасовий, а фундаментальний характер, випливаючи з базових характеристик кіберпростору та глибинних розбіжностей між державами. Транскордонність підриває традиційні концепції юрисдикції. Технологічна складність та швидкість змін перевищують можливості правового регулювання. Фундаментальні ціннісні розбіжності між демократичними та авторитарними режимами унеможливлюють консенсус з багатьох базових питань. Проблема атрибуції залишає простір для безкарності. Мультистейкхолдерний характер вимагає нових форм управління за участю недержавних акторів. Асиметрія спроможностей створює нерівні стартові умови. Балансування між безпекою та правами людини породжує складні етичні дилеми. Відсутність механізмів забезпечення виконання підриває ефективність узгоджених норм. Визнання фундаментальності цих викликів є передумовою для реалістичних очікувань та прагматичних стратегій.

Аналіз шляхів формування глобальних норм та стандартів продемонстрував, що ефективна система виникає не через один універсальний механізм, а через складну взаємодію множинних процесів. Універсальні процеси під егідою ООН забезпечують легітимність через інклюзивність. Регіональна інтеграція через ЄС або НАТО дозволяє досягати амбітніших стандартів.

Технічна стандартизація забезпечує практичну релевантність. Публічно-приватне партнерство залучає ресурси бізнесу. Механізми зміцнення довіри зменшують ризики конфліктів. Програми розвитку спроможностей підвищують глобальну стійкість. Судова практика конкретизує абстрактні норми. Механізми відповідальності створюють стимули дотримання. Освіта та дослідження забезпечують інтелектуальну основу. Адаптивне регулювання готує до майбутніх технологій. Синергія між цими механізмами створює складну екосистему нормотворення, адаптовану до різноманітності кіберпростору.

Перспективи України у глобальній системі кібербезпеки визначаються парадоксальним поєднанням екзистенційних викликів та унікальних можливостей. Російська кіберагресія створює безпрецедентний тиск, водночас генеруючи практичний досвід, високо цінований міжнародними партнерами. Імплементація європейської директиви NIS2 вимагає масштабних зусиль, проте забезпечує чіткі орієнтири та зовнішню підтримку модернізації. Потужний IT-сектор є стратегічним активом для національної безпеки. Співпраця з НАТО розвиває оперативні спроможності кібероборони. Розвиток людських ресурсів через реформування освіти забезпечує довгострокову кіберстійкість. Вдосконалення правової бази створює нормативну основу ефективного регулювання. Активне міжнародне позиціонування дозволяє трансформувати Україну з об'єкта на суб'єкт формування глобальних норм.

Вважаємо, що Україна має всі передумови для того, щоб стати визнаним центром експертизи у сфері кібербезпеки, якщо зуміє системно реалізувати наступні стратегічні пріоритети: посилення координації між державними органами через надання реальних важелів впливу Національному координаційному центру кібербезпеки; ефективна імплементація NIS2 з фокусом на найкритичніших секторах; поглиблення публічно-приватного партнерства для залучення потенціалу IT-індустрії; розвиток національних кадрів через освітні реформи та стимули для державного сектору; активна участь у міжнародних форумах для просування українських ініціатив; створення регіонального центру експертизи для позиціонування як хабу знань; систематичне документування російської агресії як доказова база майбутніх

претензій; розвиток кіберіндустрії через стратегічне партнерство та державну підтримку; формування культури кібербезпеки через освітні програми для різних аудиторій.

Проведене дослідження підтверджує гіпотезу про те, що формування ефективної глобальної системи кібербезпеки є можливим попри численні виклики, проте вимагає реалістичного розуміння обмежень міжнародної кооперації, готовності до компромісів та поступовості у нарощуванні консенсусу, інноваційних підходів до поєднання різних механізмів нормотворення та, найголовніше, політичної волі провідних держав до пріоритизації колективних інтересів глобальної кіберстійкості. Для України стратегічне завдання полягає не у пасивній адаптації до глобальних трендів, а в активному формуванні міжнародного порядку через використання унікального досвіду, побудову національних спроможностей та трансформацію з периферії у визнаний центр глобальної системи кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. ICANN та управління критичною інтернет-інфраструктурою. ІТ право: проблеми і перспективи розвитку в Україні. 2020. № 1. С. 67-79.

2. Баранов О. А. Інтернет речі і штучний інтелект: витоки проблеми правового регулювання. Інформація і право. 2018. № 2(25). С. 52-67.

3. Баранов О. А. Кіберзброя та міжнародна безпека: правові аспекти. ІТ право: проблеми і перспективи розвитку в Україні. 2019. № 1. С. 89-101.

4. Баранов О. А. Технологічна незалежність у сфері кібербезпеки: досвід Китаю. ІТ право: проблеми і перспективи розвитку в Україні. 2021. № 2. С. 123-135.

5. Гнатюк С. О. Захист промислових систем управління: уроки Stuxnet. Безпека інформації. 2018. Том 24, № 3. С. 156-167.

6. Гнатюк С. О. Кіберсуверенітет як елемент національної безпеки Китаю. Стратегічні пріоритети. 2020. № 1(53). С. 134-142.

7. Гнатюк С. О., Корченко О. Г. Індекс глобальної кібербезпеки: методологія та значення для України. Безпека інформації. 2021. Том 27, № 2. С. 78-89.

8. Гребенюк М. В. Група урядових експертів ООН: досягнення та обмеження. Актуальні проблеми міжнародних відносин. 2019. Вип. 140. С. 89-101.

9. Гребенюк М. В. Ефективність міжнародного реагування на кіберінциденти: порівняльний аналіз. Актуальні проблеми міжнародних відносин. 2021. Вип. 148. С. 89-104.

10. Гребенюк М. В. Міжнародна кібердипломатія: еволюція та сучасні тенденції. Актуальні проблеми міжнародних відносин. 2021. Вип. 147. С. 67-79.

11. Гребенюк М. В. Міжнародно-правові аспекти кіберконфліктів: проблеми атрибуції та відповідальності держав. Актуальні проблеми міжнародних відносин. 2020. Вип. 143. С. 89-104.

12. Гребенюк М. В. Перші кібервійни: естонський досвід та міжнародна реакція. Актуальні проблеми міжнародних відносин. 2018. Вип. 135. С. 112-123.

13. Гребенюк М. В. Регіональні організації та кібербезпека: порівняльний аналіз. Актуальні проблеми міжнародних відносин. 2022. Вип. 151. С. 89-103.

14. Гребенюк М. В. Український досвід кібербезпеки в контексті гібридної війни. Міжнародні відносини. 2022. № 4. С. 156-169.

15. Діордіца І. В. Атака на Colonial Pipeline: захист критичної інфраструктури США. Підприємництво, господарство і право. 2021. № 7. С. 189-195.

16. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями реалізації. Підприємництво, господарство і право. 2019. № 9. С. 173-178.

17. Діордіца І. В. Мультистейкхолдерне управління кіберпростором: перспективи розвитку. Підприємництво, господарство і право. 2022. № 8. С. 234-241.

18. Діордіца І. В. Технологічна конкуренція США та Китаю: наслідки для України. Підприємництво, господарство і право. 2020. № 7. С. 234-241.

19. Діордіца І. В. Участь України в міжнародних процесах формування норм кібербезпеки. Підприємництво, господарство і право. 2021. № 5. С. 178-185.

20. Дмитренко В. І. НАТО і кібербезпека: еволюція підходів. Стратегічні пріоритети. 2021. № 3(59). С. 112-123.

21. Дубов Д. В. Архітектура глобального кіберуправління: виклики координації. Стратегічні пріоритети. 2022. № 1(61). С. 78-89.

22. Дубов Д. В. Естонський кіберінцидент 2007 року: уроки для України. Стратегічні пріоритети. 2017. № 2(43). С. 89-97.

23. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України. Стратегічні пріоритети. 2014. № 4(33). С. 113-119.

24. Дубов Д. В. Соціальний кредит у Китаї: виклики для приватності та демократії. Інформація і право. 2020. № 2(33). С. 45-54.

25. Дубов Д. В. Українські кіберінциденти у контексті формування міжнародних норм. Стратегічні пріоритети. 2023. № 1(65). С. 89-102.

26. Дубов Д. В. Фрагментація глобального кіберпростору: ризики для міжнародної безпеки. Стратегічні пріоритети. 2021. № 2(58). С. 89-98.

27. Дубов Д. В., Ожеван М. А. Кібервійна Росії проти України: інструменти агресії. Стратегічні пріоритети. 2016. № 4(41). С. 89-105.

28. Дубов Д. В., Ожеван М. А., Гнатюк С. Л. Інформаційна безпека в умовах критичного стану суспільства. Київ: НІСД, 2011. 36 с.

29. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI (в редакції від 20.03.2020). Відомості Верховної Ради України. 2010. № 34. Ст. 481.

30. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

31. Золотар О. О. Кіберзлочинність в Україні та світі: сучасний стан та шляхи протидії. Юридичний науковий електронний журнал. 2021. № 3. С. 289-292.

32. Золотар О. О. Міжнародна конвенція ООН про кіберзлочинність: виклики та перспективи. Юридичний науковий електронний журнал. 2022. № 4. С. 267-271.

33. Золотар О. О. Північнокорейська кіберзлочинність: виклики для міжнародної безпеки. Юридичний науковий електронний журнал. 2020. № 5. С. 234-238.

34. Климчук О. О. Міжнародна допомога Україні у зміцненні кібербезпеки енергосектору. Інформація і право. 2020. № 3(34). С. 123-134.

35. Климчук О. О. Порівняльний аналіз моделей кібербезпеки провідних держав. Інформація і право. 2021. № 1(36). С. 89-101.

36. Коваль О. А. Китайська концепція управління глобальним кіберпростором. Китайські дослідження. 2020. № 1(7). С. 145-158.

37. Коваль О. А. Міжнародний союз електрозв’язку та глобальна кібербезпека. Актуальні проблеми міжнародних відносин. 2020. Вип. 144. С. 134-145.

38. Корнейко О. В. WannaCry: глобальна епідемія та уроки кібербезпеки. Науковий вісник Ужгородського національного університету. Серія: Право. 2019. Вип. 56. С. 178-183.

39. Корнейко О. В. Міжнародне співробітництво України у протидії кіберзлочинності. Науковий вісник Ужгородського національного університету. Серія: Право. 2018. Вип. 50. Т. 2. С. 123-127.

40. Корнейко О. В. Розвиток індустрії кібербезпеки: досвід США для України. Вісник Національного університету "Львівська політехніка". 2019. № 4(24). С. 112-119.

41. Корнейко О. В. Роль Інтерполу в боротьбі з транскордонною кіберзлочинністю. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Вип. 64. С. 178-183.

42. Кудряченко А. І. Документування кіберагресії: український досвід. Політичне життя. 2022. № 3. С. 67-78.

43. Кудряченко А. І. Роль ООН у формуванні норм кіберповедінки держав. Політичне життя. 2020. № 1. С. 67-75.

44. Кудряченко А. І. Трансформація глобальної системи кібербезпеки: роль нових центрів сили. Політичне життя. 2021. № 2. С. 78-87.

45. Кудряченко А. І. Формування міжнародних норм поведінки у кіберпросторі: роль України. Політичне життя. 2019. № 3. С. 89-95.

46. Ліпкан В. А. Stuxnet: нова ера кіберзброї та виклики для міжнародного права. Інформаційна безпека людини, суспільства, держави. 2011. № 2(6). С. 45-52.

47. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях. Київ: Текст, 2006. 256 с.

48. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції. Київ: КНТ, 2006. 280 с.

49. Логінов О. В. Координація міжнародного реагування на масштабні кіберінциденти. Право і безпека. 2019. № 4(75). С. 89-96.

50. Логінов О. В. Механізми міжнародної співпраці у сфері кібербезпеки: досвід для України. Право і безпека. 2020. № 2(77). С. 67-73.

51. Логінов О. В. Міжнародне правоохоронне співробітництво у кіберпросторі. Право і безпека. 2021. № 3(82). С. 89-96.

52. Макаренко Є. А. Адаптація законодавства України до acquis ЄС у сфері кібербезпеки. Міжнародні відносини: теоретико-практичні аспекти. 2021. № 7. С. 234-247.

53. Макаренко Є. А. Європейська модель кібербезпеки: уроки для України. Міжнародні відносини: теоретико-практичні аспекти. 2022. № 9. С. 201-215.

54. Макаренко Є. А. Європейська система кібербезпеки: уроки для України. Міжнародні відносини: теоретико-практичні аспекти. 2023. № 11. С. 123-137.

55. Макаренко Є. А. Роль приватного сектору у реагуванні на кіберінциденти. Міжнародні відносини: теоретико-практичні аспекти. 2021. № 8. С. 156-169.

56. Макаренко Є. А. Співробітництво НАТО та ЄС у сфері кібербезпеки. Міжнародні відносини: теоретико-практичні аспекти. 2020. № 5. С. 156-167.

57. Марущак А. І. Інституційний механізм забезпечення кібербезпеки США: досвід для України. Стратегічні пріоритети. 2018. № 3(47). С. 89-97.

58. Марущак А. І. Кібератаки на Естонію: початок нової ери конфліктів. Інформація і право. 2018. № 1(24). С. 78-86.

59. Марущак А. І. Конституційне право на інформацію в умовах кіберпростору. Інформація і право. 2017. № 3(22). С. 45-52.

60. Марущак А. І. Центр передового досвіду НАТО з кіберзахисту: досвід для України. Інформація і право. 2019. № 4(31). С. 89-98.

61. Міжнародний союз електрозв'язку. Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. Женева: ITU Publications, 2021. 136 p.

62. Ожеван М. А. Багатостороння дипломатія України у сфері кібербезпеки. Стратегічна панорама. 2023. № 1. С. 112-125.

63. Ожеван М. А. Державна політика у сфері кібербезпеки: порівняльний аналіз. Стратегічна панорама. 2017. № 2. С. 78-88.

64. Ожеван М. А. Кібератаки на енергетичну інфраструктуру України: виклики та відповіді. Стратегічна панорама. 2017. № 1. С. 78-92.

65. Ожеван М. А. Кібербезпека в контексті нових викликів національній безпеці України. Стратегічні пріоритети. 2016. № 1(38). С. 121-128.

66. Ожеван М. А. Перспективи Програми дій ООН з кібербезпеки. Стратегічна панорама. 2022. № 1. С. 89-97.

67. Ожеван М. А. Прогалини у глобальній системі кібербезпеки. Стратегічна панорама. 2020. № 2. С. 112-126.

68. Ожеван М. А. Стратегічне позиціонування України у глобальному кіберпросторі. Стратегічна панорама. 2021. № 1-2. С. 112-124.

69. Савчук К. О. Участь України у міжнародних організаціях з питань кібербезпеки. Юридичний часопис Національної академії внутрішніх справ. 2021. № 1(21). С. 156-164.

70. Ткачук Т. Ю. Будапештська конвенція про кіберзлочинність: проблеми імплементації в Україні. Право України. 2019. № 8. С. 156-168.

71. Ткачук Т. Ю. Директива NIS2: нові вимоги до кібербезпеки в ЄС. Право України. 2023. № 2. С. 201-215.

72. Ткачук Т. Ю. Правові основи кібербезпеки в Україні: стан та перспективи розвитку. Право України. 2020. № 5. С. 178-192.

73. Ткачук Т. Ю. Публічно-приватне партнерство у кібербезпеці: міжнародний досвід. Право України. 2021. № 7. С. 178-192.

74. Фурашев В. М. Правове регулювання штучного інтелекту та кібербезпеки: виклики для України. Інформація і право. 2022. № 1(40). С. 78-87.

75. Фурашев В. М. Система доменних імен: безпека та управління. Інформація і право. 2021. № 2(37). С. 45-56.

76. Шеломенцев В. П. Ransomware як загроза національній безпеці: правові аспекти. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2021. № 2(48). С. 134-145.

77. Шеломенцев В. П. Кібербезпека у системі національної безпеки України: правовий аспект. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2019. № 2(44). С. 112-123.

78. Шеломенцев В. П. Кіберспостереження як елемент національної безпеки: правові межі. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2020. № 1(45). С. 156-167.

79. Bjola C., Holmes M. (eds.) Digital Diplomacy: Theory and Practice. London: Routledge, 2015. 264 p.

80. Buchanan B. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. Oxford: Oxford University Press, 2017. 286 p.

81. Buchanan B. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. Oxford: Oxford University Press, 2017. 286 p.

82. Buchanan B. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge: Harvard University Press, 2020. 400 p.

83. Carr M. Public-private partnerships in national cyber-security strategies. International Affairs. 2016. Vol. 92, No. 1. P. 43-62.

84. Deibert R. J. Reset: Reclaiming the Internet for Civil Society. Toronto: House of Anansi Press, 2020. 280 p.

85. DeNardis L. The Global War for Internet Governance. New Haven: Yale University Press, 2014. 312 p.

86. Dunn Cavelty M. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge, 2008. 256 p.

87. Dunn Cavelty M. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge, 2008. 256 p.

88. European Union Agency for Cybersecurity. ENISA Threat Landscape 2021. Luxembourg: Publications Office of the European Union, 2021. 156 p.

89. Finnemore M., Hollis D. B. Constructing Norms for Global Cybersecurity. American Journal of International Law. 2016. Vol. 110, No. 3. P. 425-479.

90. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach. Oxford: Butterworth-Heinemann, 2014. 416 p.

91. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers. New York: Doubleday, 2019. 368 p.

92. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday, 2019. 368 p.

93. International Telecommunication Union. *Global Cybersecurity Index 2020*. Geneva: ITU Publications, 2021. 94 p.

94. International Telecommunication Union. Measuring Digital Development: Facts and Figures 2023. Geneva: ITU, 2023. 24 p.

95. International Telecommunication Union. *Overview of Cybersecurity*. Geneva: ITU, 2008. 50 p.

96. Keohane R. O., Nye J. S. Power and Interdependence. 4th ed. Boston: Longman, 2012. 334 p.

97. Lindsay J. R. Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem. Intelligence and National Security. 2017. Vol. 32, No. 7. P. 930-945.

98. Linkov I., Trump B. D., Palma-Oliveira J. M. (eds.) Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. Dordrecht: Springer, 2017. 566 p.

99. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization. Gaithersburg: NIST, 2022. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography

100. NATO. Cyber Defence Pledge. Brussels, 2016. Available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

101. Nye J. S. Cyber Power. Cambridge: Harvard Kennedy School Belfer Center, 2010. 34 p.

102. Nye J. S. Cyber Power. Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010. 34 p.

103. Nye J. S. The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series, No. 1. Waterloo: Centre for International Governance Innovation, 2014. 16 p.

104. Schmitt M. N. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017. 598 p.

105. Shackelford S. J. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge: Cambridge University Press, 2014. 396 p.

106. Shackelford S. J., Russell S., Kuehn A. Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. Chicago Journal of International Law. 2017. Vol. 17, No. 1. P. 1-50.

107. Shen Y. Cyber Sovereignty and the Governance of Global Cyberspace. Chinese Journal of International Law. 2016. Vol. 15, No. 1. P. 1-25.

108. Sophos. The History of Cybercrime 1990-2000. Technical Report. 2020. Available at: https://www.sophos.com/en-us/security-news-trends

109. Tikk E., Kaska K., Vihul L. International Cyber Incidents: Legal Considerations. Tallinn: NATO CCD COE, 2010. 103 p.

110. Valeriano B., Maness R. C. Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press, 2015. 288 p.

111. Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishers, 2014. 448 p.

АНОТАЦІЯ

Третяк В. Д. Міжнародна політика забезпечення кібербезпеки: пошук глобальних стандартів (магістерська робота). Харків: Харківський національний університет імені В. Н. Каразіна, 2025.107 с. (рукопис).

Мета дослідження полягає у виявленні закономірностей формування глобальних стандартів у сфері кібербезпеки, визначенні ключових викликів та перешкод у цій сфері, а також обґрунтування стратегічних пріоритетів інтеграції України у міжнародну систему кіберзахисту.

Об'єкт дослідження є міжнародна політика у сфері кібербезпеки.

Предметом дослідження є процеси формування глобальних норм та стандартів політики міжнародної кібербезпеки.

У першому розділі розглянуто теоретичні засади дослідження міжнародної кібербезпеки. Проаналізовано еволюцію концепту кібербезпеки, сучасні наукові підходи до формування політики у сфері кіберзахисту, а також міжнародно-правові засади регулювання кіберпростору. Особлива увага приділяється взаємодії традиційних теорій міжнародних відносин із новими концепціями цифрової безпеки й оцінці нормативної бази, що регулює використання інформаційно-комунікаційних технологій у глобальному вимірі.

У другому розділі досліджено сучасну міжнародну політику забезпечення кібербезпеки. Проведено порівняльний аналіз стратегій провідних держав, насамперед США та Китайської Народної Республіки, окреслено пріоритети їхнього кіберуправління та ключові нормативні документи з регулювання кіберпростору. Розглянуто діяльність міжнародних організацій, зокрема ООН, НАТО, ITU, ICANN та INTERPOL, проаналізовано їхній внесок у формування архітектури глобальної кібербезпеки та проблеми координації між різними акторами. Окрему увагу приділено аналізу конкретних кіберінцидентів як практичного виміру ефективності міжнародної співпраці у сфері реагування на кіберзагрози.

У третьому розділі визначено перспективи формування глобальних стандартів кібербезпеки. Виявлено ключові виклики міжнародного регулювання кіберпростору, оцінено потенціал глобальних ініціатив, включаючи діяльність Групи урядових експертів ООН та Паризький заклик. Сформульовано пропозиції щодо створення дієвої багаторівневої моделі глобального управління кібербезпекою та обґрунтовано можливості її адаптації для України з метою посилення національного кіберзахисту й активізації участі у міжнародних кіберпроцесах.

Ключові слова: кібербезпека, кіберпростір, міжнародні організації, кіберзагрози, глобальні стандарти, міжнародне право, США, Китай, кіберрегулювання.

ANNOTATION

Tretiak V. D. International Cybersecurity Policy: The Search for Global Standards (Master's thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 107 p. (manuscript).

The aim of the study is to identify the patterns of forming global standards in the field of cybersecurity, determine key challenges and obstacles in this area, and substantiate strategic priorities for Ukraine's integration into the international cybersecurity system.

The object of the research is international policy in the field of cybersecurity.

The subject of the research is the processes of forming global norms and standards of international cybersecurity policy.

The first section examines the theoretical foundations of researching international cybersecurity. It analyses the evolution of the cybersecurity concept, contemporary academic approaches to policy-making in the field of cyber protection, as well as international legal frameworks for regulating cyberspace. Particular attention is paid to the interaction between traditional theories of international relations and new concepts of digital security, along with the assessment of the regulatory framework governing the use of information and communication technologies in the global dimension.

The second section explores contemporary international cybersecurity policy. A comparative analysis of strategies of leading states, primarily the United States and the People's Republic of China, is carried out, outlining the priorities of their cyber governance and key regulatory documents for governing cyberspace. The activities of international organizations, including the UN, NATO, ITU, ICANN, and INTERPOL, are examined, with an assessment of their contribution to shaping the architecture of global cybersecurity and the problems of coordination among different actors. Special attention is devoted to analysing specific cyber incidents as a practical reflection of the effectiveness of international cooperation in responding to cyber threats.

The third section defines the prospects for forming global cybersecurity standards. It identifies key challenges of international regulation of cyberspace and assesses the potential of global initiatives, including the work of the UN Group of Governmental Experts and the Paris Call. The section formulates proposals for establishing an effective multi-level model of global cybersecurity governance and substantiates the possibilities of adapting it to Ukraine in order to strengthen national cyber protection and increase participation in international cyber processes.

Keywords: cybersecurity, cyberspace, international organizations, cyber threats, global standards, international law, USA, China, cyber regulation.

ВІДГУК

наукового керівника на кваліфікаційну роботу магістра
студента 2-го року навчання, другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОПП «Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин»
Харківського національного університету імені В.Н. Каразіна
Третяка Віталія Дмитровича
на тему:
«Міжнародна політика забезпечення кібербезпеки: пошук глобальних стандартів»

Кваліфікаційна робота магістранта Третяка Віталія Дмитровича присвячена комплексному аналізу процесів формування міжнародної політики у сфері кібербезпеки, дослідженню викликів глобального регулювання кіберпростору та визначенню стратегічних пріоритетів України в умовах сучасних кіберзагроз. Тема роботи є надзвичайно актуальною та має важливе теоретичне й практичне значення, особливо з огляду на гібридну агресію проти України та зростання ролі кіберпростору у міжнародних відносинах.

Автором продемонстровано вміння працювати з сучасними науковими джерелами, міжнародно-правовими документами та матеріалами провідних міжнародних організацій. Структура роботи є логічною та відповідає вимогам до магістерських досліджень. У роботі поєднано теоретичний аналіз, елементи порівняльного аналізу, інституційний підхід та методи кейс-стаді, що дозволило автору отримати змістовні висновки та запропонувати аргументовані рекомендації.

До сильних сторін роботи слід віднести ґрунтовний огляд еволюції поглядів на кібербезпеку в міжнародних відносинах, детальний аналіз політик США, ЄС та інших ключових акторів, об’єктивний розгляд ролі міжнародних організацій і процесів нормотворення, уважний аналіз українського досвіду протидії кіберзагрозам, а також чітко сформульовані висновки й практичні пропозиції.

Разом з тим, у ході підготовки роботи було виявлено кілька аспектів, які доцільно вдосконалити, зокрема недостатнє застосування порівняльних таблиць і схем для структуризації підходів різних держав і міжнародних організацій, недостатня кількість узагальнених висновків за кожним кейсом. Зазначені зауваження не є критичними та не знижують загальної позитивної оцінки роботи. Вони мають характер побажань та відображають перспективи подальшого розвитку теми.

У цілому кваліфікаційна робота магістранта Третяка Віталія Дмитровича є самостійним, ґрунтовним та якісно виконаним дослідженням, яке відповідає вимогам, встановленим до магістерських робіт зі спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Робота заслуговує на високу оцінку (92А) та може бути рекомендована до захисту перед екзаменаційною комісією.

Науковий керівник:
Кандидат політичних наук, доцент
Професор кафедри міжнародних відносин **Ольга ВИГОВСЬКА**

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го року навчання, другого (магістерського) рівня вищої освіти, спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», ОПП «Міжнародні відносини, суспільні комунікації та регіональні студії»
ННІ «Каразінський інститут міжнародних відносин»
Харківського національного університету імені В.Н. Каразіна
Коваленка Романа Сергійовича
на тему:
««Зовнішня політика України: між євроатлантичними прагненнями та викликами воєнної реальності»

Кваліфікаційна робота присвячена комплексному аналізу трансформації зовнішньої політики України в умовах повномасштабної війни, зміни міжнародної безпекової системи та посилення стратегічного значення євроатлантичного курсу. Актуальність теми очевидна, Україна перебуває в епіцентрі глобальних політичних процесів, які визначають архітектуру безпеки у XXI столітті, а її зовнішня політика зазнає безпрецедентної еволюції під впливом воєнних, політичних та геостратегічних факторів. Автор переконливо обґрунтовує, що війна стала каталізатором глибокої модернізації міжнародної суб'єктності України, змінила формати співпраці з НАТО та ЄС і зумовила появу нових інструментів двосторонніх гарантій безпеки.

Структура роботи логічна, послідовна та відповідає вимогам до магістерських досліджень. У першому розділі автор детально розглядає теоретичні підходи та внутрішні й зовнішні фактори формування зовнішньої політики України, наголошуючи на їх багатогранності та взаємозалежності, зокрема ролі політичної системи, громадської думки, міжнародних акторів та змін у глобальному балансі сил

У другому розділі приділено увагу розвитку партнерства з НАТО, аналізу рішень Вільнюського саміту 2023 року та появі Ради Україна–НАТО, що суттєво інституціоналізувало співпрацю сторін. Автор ґрунтовно висвітлює двосторонні безпекові угоди України з провідними державами світу, започатковані у 2024 році, як новий формат гарантій під час війни. У третьому розділі досліджено еволюцію відносин України та Європейського Союзу, підкреслено значення статусу кандидата й нової динаміки інтеграційного процесу в умовах війни.

Наукова новизна роботи полягає у комплексному аналізі взаємодії між євроінтеграційним та євроатлантичним напрямами зовнішньої політики України в умовах війни, а також у виявленні нових дипломатичних інструментів, що сформувалися після 2022 року. Автор застосовує теоретичні підходи, що поєднують системний, інституційний та діяльнісний аналіз, демонструючи здатність критично осмислювати сучасні міжнародно-політичні процеси.

Практична значущість роботи визначається її можливістю бути використаною у сфері стратегічного планування зовнішньої політики України, формуванні довгострокових рішень щодо співпраці з НАТО та ЄС, оцінці ефективності нових форматів гарантій безпеки, а також у навчальному процесі під час викладання курсів із міжнародних відносин, зовнішньої політики та європейської інтеграції.

Разом з тим, робота могла б бути посилена шляхом ширшого застосування порівняльних таблиць для систематизації підходів НАТО та ЄС до безпекової взаємодії з Україною, а також більш детального аналізу окремих кейсів підтримки,

зокрема в енергетичній та оборонній сферах. Такі зауваження носять рекомендаційний характер і не впливають на загальну позитивну оцінку дослідження.

Кваліфікаційна робота Коваленка Романа Сергійовича є змістовним, якісним та самостійно виконаним дослідженням, що повністю відповідає вимогам, встановленим до магістерських робіт зі спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Робота відзначається високим рівнем аналітики, академічною культурою, логічністю викладу та актуальністю висновків. Дослідження заслуговує на високу оцінку (A, 92 бали) та може бути рекомендоване до захисту перед екзаменаційною комісією.

Рецензент:
кандидат політичних наук,
завідувачка кафедри міжнародної інформації
Навчально-наукового інституту міжнародних відносин
Київського національного університету
імені Тараса Шевченка **Наталія БЄЛОУСОВА**