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: **«ГЛОБАЛЬНІ ВИКЛИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У XXI СТОЛІТТІ»**

Виконав:
студент 2-го курсу, групи УМІБ-61
другого (магістерського) рівня вищої освіти,
спеціальності 291 «Міжнародні відносини, суспільні
комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Кочанов Володимир Валерійович

Керівник:
д. політ.н., завідувач кафедри міжнародних відносин, Вінникова Наталія Анатоліївна

Рецензент:
к. соціол. н., доц.
Нікулін В’ячеслав Сергійович

ХАРКІВ – 2025 р.

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

ЗАТВЕРДЖУЮ
завідувач кафедри

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

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

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Кочанова Володмимира Валерійовича
(прізвище, ім'я та по батькові)

1. Тема роботи «Глобальні виклики інформаційної безпеки у XXI столітті» керівник роботи д.політ.н., доц. Вінникова Наталія Анатоліївна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» червня 2025 року № 400-5/1324(зі змінами від «10» вересня 2025 року № 4001-5/3049; «6» жовтня 2025 року№ 4001-5/3656.

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

3. Перелік питань, які потрібно розробити:

Сутність та еволюція поняття « міжнародна інформаційна безпека» в теорії міжнародних відносин

1. Ключові технології XXI століття та їх вплив на міжнародну інформаційну безпеку.
2. Ризики, пов'язані з використанням штучного інтелекту.
3. Стратегії державного реагування на виклики, зумовлені розвитком цифрових технологій, включаючи ШІ.
4. Роль кібердипломатії у забезпеченні інформаційної безпеки.

5. Міжнародні ініціативи та багасторонні форми співпрації в умовах трансформації цифрових технологій.

6. Положення України в площині кібердипломатії та міжнародних відносин в епоху розвитку цифрових технологій.

7. Перспективи глобального нормативного консенсусу у сфері цифрових технологій.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

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

Здобувач вищої освіти _____ Володимир КОЧАНОВ
(підпис) (ім'я, прізвище)

Керівник роботи _____ Наталія ВІННИКОВА
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Технології на основі штучного інтелекту створюють значні ризики для глобального інформаційного середовища. Основні ризики включають кібершпигунство, масові витоки даних, випадки крадіжки особистих даних, фішинг та високотехнологічні кібератаки [11; 16; 17; 90]. На додачу до цих технічних загроз, ШІ все частіше використовується в інформаційній війні, поширюючи конфлікт на інформаційну сферу та дестабілізуючи суспільства за межами поля бою. Яскравим прикладом є використання Росією технологій deepfake, зокрема сфабрикованих відеороликів з президентом України Володимиром Зеленським, що мають на меті підірвати довіру громадськості та маніпулювати національною думкою [84]. Подібні інциденти наочно демонструють, як ШІ може бути використаний як зброя для політичного впливу, що призводить до зростання міжнародної нестабільності.

В епоху стрімкого технологічного прогресу інформаційна безпека стала одним із визначальних викликів цифрової трансформації. У міру розширення цифрових екосистем держави, організації та суспільства стикаються з подвійним викликом: сприяти інноваціям і водночас підтримувати стабільність та стійкість інформаційного середовища. Згідно з останніми дослідженнями, діджиталізація критичної інфраструктури та інтеграція штучного інтелекту, хмарних технологій та Інтернету речей змінили не тільки технічні, а й стратегічні аспекти кібербезпеки [85].

Дослідження останніх років висвітлюють як технологічні, так і управлінські ризики, що виникають у результаті цифрової трансформації. Українські науковці, серед яких І. Арістова [1], О. Баранов [3], К. Бєляков [4], І. Боднар [5], В. Гавловський [8], М. Гаврильців [9], Б. Кормич [20], та інші — підкреслюють, що прискорення цифрових процесів у державній адміністрації, економіці та освіті супроводжується підвищеною вразливістю до кіберзагроз, витоків даних та дезінформаційних кампаній. Хоча цифрові технології підвищують ефективність та доступність, вони також створюють системні

вразливості, які неможливо усунути виключно за допомогою технічних рішень. Як зазначає Раданлієв [85], для ефективного реагування необхідний підхід «цифрової безпеки за замовчуванням», що передбачає інтеграцію технологічних, етичних та соціальних аспектів на ранніх етапах розробки системи.

Ще однією темою академічних дискусій є баланс між інноваціями та регулюванням. Багато авторів стверджують, що цифрова трансформація вимагає не тільки технологічних розробок, а й узгодження національних та міжнародних нормативних рамок [20; 80; 81; 88]. Приведення стратегій кібербезпеки на державному рівні у відповідність до міжнародних стандартів, таких як ISO/IEC 27001 та Директива ЄС NIS 2, залишається центральним викликом у сучасних дискусіях. Вчені також наголошують на зростаючій актуальності гібридних загроз, що поєднують кібератаки з цілеспрямованими інформаційними операціями, які стали особливо очевидними в контексті України.

З огляду на ці виклики, **метою** дослідження є визначення впливу сучасних викликів на міжнародну інформаційну безпеку. Для досягнення цієї мети в рамках дослідження будуть поставлені такі **завдання**:

- Визначити ключові технологічні тенденції, що впливають на стан інформаційної безпеки.
- З’ясувати основні вектори загроз та оцінити стратегії держав реагування на них.
- Встановити ризики, які штучний інтелект становить для системи інформаційної безпеки.
- Запропонувати заходи протидії цим загрозам через міжнародну співпрацю та дипломатичні механізми.

Об'єктом цього дослідження є глобальна безпека міжнародної інформаційної безпеки. **Предметом** цього дослідження є сучасні виклики міжнародної інформаційної безпеки.

У дослідженні застосовується метод компаративного аналізу для виявлення сучасних тенденцій, оцінки ефективності національних та міжнародних стратегій, а також перспектив розвитку скоординованої глобальної архітектури інформаційної безпеки. За допомогою методу аналізу документів досліджено міжнародну нормативну базу з питань інформаційної безпеки. Такий підхід дозволяє отримати детальне комплексне розуміння того, як держави та міжнародні інституції реагують на нові цифрові загрози, прагнучи створити безпечні та стійкі інформаційні системи.

У міру прискорення цифрової трансформації міжнародної системи інформаційна безпека стає як передумовою, так і наслідком сталого розвитку. Тому для формування ефективних державних і міжнародних стратегій, що забезпечують стабільність, прозорість і безпеку в цифрову епоху, надзвичайно важливо розуміти ризики, пов'язані зі штучним інтелектом та пов'язаними з ним технологіями.

Перспективи подальшого дослідження полягають у поглибленому аналізі міжнародних механізмів регулювання штучного інтелекту та цифрових технологій, розробці моделей етичного і правового управління інформаційною безпекою, а також у порівняльному вивченні національних стратегій держав у сфері кіберзахисту. Такі дослідження сприятимуть формуванню універсальних стандартів цифрової стійкості й удосконаленню глобальної архітектури інформаційної безпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЦИФРОВУ ЕПОХУ

Питання інформаційної безпеки постійно залишається на порядку денному міжнародних відносин. У світлі процесів глобалізації, трансформації міжнародної системи та характеру загроз, сучасна система колективної безпеки також зазнає значних змін. У цьому розділі ми розглянемо поняття та еволюцію міжнародної безпеки, зокрема роль цифрових технологій у формуванні сучасного стану глобальної інформаційної безпеки.

1.1. Поняття та еволюція міжнародної інформаційної безпеки

Міжнародна інформаційна безпека зазнала трансформації від вузького розуміння технічного захисту до широкого, багатовимірного поняття, що інтегрує політичну стабільність, соціальну стійкість та цифрове врядування. На початку періоду після холодної війни інформаційна безпека зосереджувалася переважно на захисті державних систем зв'язку від шпигунства та запобіганні зловживанню інформаційними інфраструктурами. Утім, із стрімким розвитком інтернету, зростанням глобальної взаємопов'язаності та появою нових інструментів впливу — від кібератак до масштабних кампаній з дезінформації — міжнародна спільнота почала визнавати інформаційну безпеку основою глобальної стабільності.

Інформаційна безпека посідає центральне місце у системі міжнародної безпеки XXI століття, адже інформація стала стратегічним ресурсом, який визначає політичну стабільність, економічний розвиток і соціальну згуртованість держав. З переходом людства до цифрової епохи інформація перетворилася на самостійний інструмент впливу, а її захист - на ключовий чинник національної стійкості. Це призвело до формування нового виміру безпеки, який доповнює традиційні воєнні, політичні та економічні складові глобальної системи. Як наслідок, держави все частіше сприймають

інформаційну безпеку як невід'ємну складову національного суверенітету та визначальний фактор їхнього положення в міжнародній системі.

Починаючи з другої половини XX століття, інформаційна безпека розглядалася переважно як елемент національної оборони. Проте з розвитком технологій і зростанням ролі комунікацій у міжнародних відносинах, її трактування поступово розширилося — від технічного захисту інформаційних систем до комплексного політико-правового та соціального явища. Саме тому сучасне розуміння інформаційної безпеки включає не лише запобігання несанкціонованому доступу до даних, але й підтримання цілісності, достовірності та доступності інформаційного простору.

Інформація, як глобальне явище, створює складні проблеми в міжнародній інформаційній сфері. Ця сфера охоплює національні інформаційні поля, кожне з яких держави намагаються регулювати відповідно до своїх правових традицій, культурних звичаїв та соціальних норм. Інформаційна безпека, як один із ключових факторів міжнародних відносин, чинить універсальний вплив на поведінку широкого кола суб'єктів міжнародної системи [26]. З огляду на глобальний характер інформаційної безпеки, багато розвинених країн ініціювали довгострокові державні програми, спрямовані на забезпечення захисту критичної інформаційної інфраструктури.

У загальному розумінні інформаційна безпека є станом захисту інформації, систем та середовищ, в яких зберігаються конфіденційність, цілісність та доступність даних. Ця тріада лежить в основі усіх сучасних підходів до управління безпекою [13; 19].

Конфіденційність передбачає, що доступ до інформації мають лише уповноважені особи. Цілісність гарантує, що дані залишаються точними та незмінними, якщо вони не змінюються законним шляхом. Доступність дозволяє за потреби уповноваженим користувачам отримувати доступ до інформації. Ці три принципи, спочатку закріплені в таких стандартах, як ISO/IEC 27001 та

ISO/IEC 27002, залишаються універсальними орієнтирами для захисту інформації як у державному, так і в приватному секторах (ISO/IEC, 2022) [21].

Поняття інформаційної безпеки охоплює кілька рівнів - особистий, інституційний та національний. Воно об'єднує безпеку як цифрових, так і нецифрових носіїв інформації, включаючи друковані документи, усне спілкування та будь-які форми передачі даних. Відтак, інформаційну безпеку слід розуміти не лише як технологічну проблему, а як системну дисципліну, що спрямована на захист усіх інформаційних активів у соціальному та політичному контексті. Такі дослідники, як І. Арістова та Б. Кормич, наголошують, що інформаційна безпека є функціональною складовою національної безпеки, яка формує стійкість держави, соціальну довіру та захист суверенітету в інформаційну епоху [1; 20].

Ключовим аналітичним аспектом є взаємозв'язок між інформаційною безпекою та кібербезпекою. Незважаючи на те, що ці два терміни часто вживаються як тотожні, їхня сфера застосування та мета відрізняються.

Еволюція поняття інформаційної безпеки відбувалася паралельно з розвитком кібербезпеки. Інформаційна безпека є більш широким поняттям, що охоплює захист усіх форм інформації, незалежно від носія, на якому вона зберігається. Натомість кібербезпека є підкатегорією інформаційної безпеки, що зосереджується конкретно на цифрових та мережевих середовищах — комп'ютерних системах, Інтернеті, телекомунікаціях та хмарних інфраструктурах. Її основним завданням є захист електронної інформації від таких загроз, як зловмисне програмне забезпечення, фішинг, порушення безпеки даних та атаки типу « DDoS» [55; 75; 77].

Таким чином, кібербезпека доповнює та посилює інформаційну безпеку, поширюючи її захисні механізми на цифрове середовище. Інформаційна безпека охоплює всі аспекти захисту даних, включаючи фізичні, організаційні та

юридичні, тоді як кібербезпека забезпечує цей захист у сфері комп'ютерних мереж і систем, запобігаючи кібератакам, витоку даних та технічним збоям.

Відповідно до ISO/IEC [66; 67; 68] та NIST [75; 76], кібербезпека захищає цифрову інфраструктуру шляхом впровадження технічних заходів захисту, включаючи фаєрволи, антивірусні системи, протоколи шифрування та сегментування мережі. Ці механізми забезпечують конфіденційність та цілісність систем зв'язку, баз даних та пристроїв користувачів, які обробляють або зберігають інформацію.

Європейське агентство з кібербезпеки наголошує на необхідності забезпечення можливостей виявлення та реагування в режимі реального часу, таких як аналіз мережевого трафіку, системи виявлення вторгнень та автоматизовані інструменти моніторингу [55]. Ці засоби дозволяють організаціям виявляти та протидіяти атакам, які традиційні заходи інформаційної безпеки можуть не виявити.

Згідно з останніми дослідженнями, штучний інтелект (ШІ) та машинне навчання все частіше залучаються до операцій з кібербезпеки. Дослідження Брандажа та ін. [43, с.36-37] та OECP [82; 83] показують, що системи на основі ШІ можуть обробляти великі обсяги даних з метою виявлення прихованих взаємозв'язків, розпізнавання аномалій та передбачення нових загроз, тим самим підвищуючи загальну стійкість цифрових середовищ.

З огляду на це, кібербезпека є практичним і технологічним доповненням інформаційної безпеки. Вона не тільки зберігає цифрову інформацію, але й забезпечує безперебійне функціонування інфраструктур, через які ця інформація поширюється. Завдяки інтеграції технічних механізмів захисту з розширеними системами управління кібербезпека робить всю систему інформаційної безпеки більш динамічною, адаптивною та ефективною.

Взаємозалежність між цими двома напрямками свідчить про важливу еволюцію сучасного уявлення про безпеку — починаючи від захисту ізольованих сховищ даних і закінчуючи забезпеченням цілісності та функціональності взаємопов'язаних інформаційних систем на всіх рівнях. Такий цілісний підхід є надзвичайно важливим у XXI столітті, коли межа між інформаційною та кіберсферою фактично зникла. Забезпечення інформаційної безпеки сьогодні означає забезпечення кібербезпеки — і навпаки — в умовах комплексної системи правових норм, технологічних стандартів та практик співпраці.

Ця взаємодія також сформувала сучасне міжнародне розуміння інформаційної безпеки. У рамках адаптації міжнародного права до стрімкого розвитку суспільства та інформаційних технологій поступово встановлюються універсальні принципи формування, планування та реалізації державної політики у сфері інформаційної безпеки за допомогою інструментів Організації Об'єднаних Націй.

У 1996 році питання міжнародної інформаційної безпеки було вперше формально поставлено на політичний і правовий рівень. У цьому ж році поняття міжнародної інформаційної безпеки обговорювалося на міжнародній конференції з проблем визначення інформаційного суспільства і глобальної цивілізації (ПАР, 1996) [72, с.133]. У 1997 році загроза розробки інформаційної зброї була підкреслена у спільному комюніке на найвищому рівні між росією та США [91]. Пізніше, під час 52-ї сесії Генеральної Асамблеї Організації Об'єднаних Націй, була прийнята Резолюція 53/70 від 4 грудня 1998 року. Ця резолюція визнала інформаційну безпеку багатогранною стратегічною сферою співпраці між державами. З того часу питання нових технологій у контексті міжнародної безпеки щорічно порушується на Першому комітеті Організації Об'єднаних Націй [97; 98; 99].

Питання міжнародної інформаційної безпеки залишається актуальним і на сьогоднішній день. У 2018 році Організація Об'єднаних Націй створила Робочу групу відкритого складу з питань розвитку в галузі інформації та телекомунікацій у контексті міжнародної безпеки (OEWG). Ця група була створена з метою розширення дискусій, які раніше проводилися в рамках Групи урядових експертів ООН (UNGGE), за участі всіх 193 держав-членів ООН. У період з 2019 по 2020 рік OEWG провела три суттєві засідання. Хоча як OEWG, так і остання UNGGE мали мандат на вирішення питань безпеки на міждержавному рівні, їхні повноваження також включали критично важливе завдання з'ясувати, як міжнародне право застосовується до використання інформаційних і телекомунікаційних технологій. Хоча це питання було предметом суперечок з початку обговорень в ООН у 1998 році, значний прогрес був досягнутий лише в рамках UNGGE у 2012–2013 та 2014–2015 роках, а також під час зборів 1-го Комітету Генеральної Асамблеї у 2018 році [96; 97; 98; 99].

На національному рівні протягом 2010-х років багато держав ухвалили нові закони та стандарти з метою протидії наростаючим загрозам. Одним із найвизначніших прикладів стало прийняття Закону про захист персональних даних, який набрав чинності у 2018 році.

Однак, незважаючи на все вище зазначене, виклики інформаційної безпеки набули нових масштабів із швидким поширенням штучного інтелекту та інших цифрових технологій, що додатково ускладнилося використанням таких інструментів росією в ході повномасштабної війни проти України, яка триває з 2022 року. Інформаційні інструменти на території Росії поширювалися через різні канали комунікації [84] й досі не втрачають активності, а навпаки — набирають нових обертів, що створює додаткові труднощі для ефективної протидії їм.

Отже, можна дійти висновку, що інформаційна безпека є не лише предметом технічного регулювання, але й наразі виступає політичним

інструментом. Вона визначає стратегічні відносини між державами, впливає на формування міжнародного права в цифровій сфері й стає невід'ємним елементом глобальної архітектури миру та стабільності. Відповідно, її вивчення у контексті цифрових технологій дає змогу оцінити не лише технічні аспекти, а й системні зміни в безпековому мисленні XXI століття.

1.2. Цифрові технології як фактор трансформації безпекових парадигм

XXI століття відзначається прискореним технологічним прогресом, який докорінно змінює глобальну безпеку. Штучний інтелект, Інтернет речей, хмарні обчислення, блокчейн, мережі 5G та квантові технології стали основними рушіями економічного розвитку та управління, одночасно розширюючи глобальну площину атак.

Розвиток цифрових технологій у XXI столітті докорінно змінив уявлення про природу безпеки, її структуру та методи забезпечення. Якщо у минулому безпека асоціювалася переважно з воєнними, політичними чи економічними аспектами, то нині вона набула комплексного, багатовимірного характеру. Цифровізація охопила практично всі сфери суспільного життя [32] — від управління державою до особистих комунікацій — що перетворило інформаційний простір на ключову арену сучасних конфліктів і конкуренції.

Ці технології прискорили потік інформації та збільшили залежність суспільства від цифрової інфраструктури, що призводить до набагато серйозніших наслідків, ніж у попередні десятиліття. Критична інфраструктура — від енергетичних і транспортних систем до охорони здоров'я, фінансів та державного управління — тепер функціонує на взаємопов'язаних мережах, що одночасно підвищує ефективність і водночас робить держави вразливими до нових загроз. Як результат, Цифрові технології створили передумови для переходу від традиційної концепції оборони до нової, "інформаційно орієнтованої" парадигми безпеки. У цій системі головним об'єктом захисту є не лише територія чи ресурси, а й інформація — як стратегічний актив держави. Ця

еволюція є глибоким зрушенням: цифровізація змінила не тільки те, як суспільства генерують і обробляють інформацію, але й те, як розподіляються влада, вплив і вразливість у міжнародній системі [1].

Водночас, поряд із цими перевагами, цифрова трансформація створює нові вразливі місця, особливо у сфері національної та міжнародної безпеки. Держави все частіше стикаються з кіберзагрозами, кіберзлочинністю, кібервійною, кібершпигунством, кібертероризмом та кібератаками, спрямованими проти критичної інфраструктури, національної оборони, державного управління, виборчих систем та персональних даних [86].

У основі цієї трансформації лежать інформаційно-комунікаційні технології (ІКТ), IoT, штучний інтелект (ШІ), великі дані та блокчейн. Ці новітні інструменти не тільки забезпечують моніторинг ризиків у режимі реального часу, але й дозволяють моделювати загрози, що робить цифрове передбачення важливою складовою національної та міжнародної безпеки. Однак, як зазначає Джозеф С. Най, поширення цих технологій перерозподіляє владу між державами, корпораціями та окремими особами, створюючи нові асиметрії та вразливі місця. Кібермогутність — здатність досягати бажаних результатів за допомогою цифрових ресурсів — стала визначальною рисою сучасної геополітики [80, с.3].

Ці зміни трансформують традиційні парадигми безпеки, створюючи виклики, що виходять за межі кордонів, вимагають швидкої адаптації та розмивають межу між військовою та цивільною сферами. Класичні підходи до захисту суверенітету та територіальної цілісності вже не є достатніми; натомість нові стратегії повинні інтегрувати кібербезпеку, цифрову дипломатію та стійкість критичної інфраструктури [92]. Більше того, цифрові інструменти все частіше використовуються для зміцнення національних оборонних можливостей, що вимагає як технічних інновацій, так і підвищення цифрової грамотності громадян [98].

Зрушення парадигми також простежується у зміні характеру влади та взаємозалежності. За словами Найє, цифрова зв'язність створює форму складної взаємозалежності, в якій традиційні механізми стримування вже не є достатніми. Держави тепер мусять орієнтуватися в мережі асиметричних вразливостей, де недержавні актори, приватні корпорації і навіть окремі особи можуть чинити вплив, який раніше був притаманний лише державам. У цифрову революцію влада здійснюється не стільки через примус, скільки через контроль доступу, коду та інформації [81, с. 1-2].

Цифрові технології кардинально змінили поняття інформаційної безпеки. З одного боку, вони забезпечують швидкий обмін досвідом, розвиток цифрової економіки та розширення глобальних комунікаційних мереж, але з іншого боку, створюють безпрецедентні виклики для стабільності інформаційного простору. Розвиток штучного інтелекту (ШІ), машинного навчання та аналізу великих даних значно ускладнює завдання відрізнити справжню інформацію від хибної, що підриває довіру до інформаційних систем та інституцій. [43, с.10].

Низка значних змін відбулася у сфері дезінформації. Інструменти на основі штучного інтелекту дозволяють масово створювати фальшивий контент, зокрема дипфейки, синтетичний аудіоконтент та текст, згенерований алгоритмами, які можуть використовуватися для маніпулювання громадською думкою, втручання у демократичні процеси та дестабілізації суспільства. [84]. Окрім того, цифрові технології спричиняють більшу вразливість особистих та організаційних даних. Кібершпигунство та порушення безпеки даних, спрямовані проти державних установ, критичної інфраструктури та приватних корпорацій, наразі становлять системні ризики для національної та міжнародної інформаційної безпеки. За даними Міжнародного союзу електрозв'язку (2021), понад 80 % держав повідомили про значне збільшення кількості інцидентів, пов'язаних з даними, у період з 2018 по 2021 рік, що підкреслює глобальний масштаб цієї проблеми [99].

Цифровізація також змінює інституційний вимір інформаційної безпеки. Виборчі системи, державні адміністрації та медіа-екосистеми дедалі більше цифровізуються, що робить їх більш ефективними, але водночас і більш вразливими. Атаки на виборчі процеси, маніпулювання алгоритмами соціальних мереж та скоординовані кампанії з дезінформації демонструють, що інформаційний суверенітет може бути підірваний без перетину територіальних кордонів [86].

Зміна безпекових парадигм проявляється також у переосмисленні ролі інформаційної безпеки: від захисту інформаційних систем — до управління довірою, репутацією та стабільністю інформаційного середовища. Цифрові технології не лише розширили канали комунікації, а й ускладнили ідентифікацію достовірності інформації, що створює ґрунт для маніпуляцій, фейкових наративів і підриву суспільної згуртованості [43, с.6; 84].

Традиційні підходи, зосереджені на захисті фізичної інфраструктури, тепер повинні доповнюватися стратегіями, спрямованими на захист інформаційної цілісності, стійкості до дезінформації та транскордонного співробітництва для боротьби з маніпуляціями в кіберпросторі [92].

Таким чином, цифрові технології виступають подвійним чинником у сфері безпеки — вони водночас зміцнюють і ускладнюють її. Нові інструменти управління ризиками дають змогу ефективніше виявляти загрози, але також створюють нові вектори атак. Зміна парадигми безпеки відображає перехід від традиційних оборонних концепцій до інтегрованих цифрових стратегій, у яких інформація стає головним ресурсом, а довіра — ключовим елементом міжнародної стабільності.

1.3. Методологічні підходи дослідження інформаційних ризиків

Швидкий розвиток цифрових технологій, глобальна взаємозалежність інформаційних систем і поява нових типів загроз зумовили необхідність наукового переосмислення підходів до аналізу ризиків у сфері інформаційної

безпеки. Сучасне інформаційне середовище характеризується високим рівнем динамічності, невизначеності та комплексності, що ускладнює застосування традиційних методів оцінювання небезпек. Тому виникла потреба у формуванні міждисциплінарної методологічної бази, яка б дозволила інтегрувати технічні, правові, економічні, політичні та соціальні аспекти інформаційної безпеки.

У цьому контексті аналіз інформаційних ризиків розглядається як процес виявлення, оцінки та моніторингу потенційних загроз — як зловмисних, так і випадкових — та їх впливу на інформаційні системи та дані. Його основною метою є зменшення ймовірності витоку інформації або ж порушення її неушкодженості. Цей процес включає виявлення ризиків, оцінку їх впливу та ймовірності, а також розробку заходів для зменшення або усунення загроз. Такі заходи повинні бути інтегровані в більш широку систему управління, на організаційному, національному чи міжнародному рівні [42; 66; 67; 76].

У цьому дослідженні визначено чотири методологічні підходи, які є найбільш релевантними для аналізу ризиків у сфері інформаційної безпеки:

- **Стратегічно-комунікативний підхід.** Цей підхід орієнтований на моніторинг та аналіз інформаційного простору з метою виявлення інформаційно-психологічного впливу (ІПВ). Він передбачає класифікацію повідомлень, аналіз настроїв та семантичний аналіз, а також вивчення наративів. Такі методи дозволяють виявляти загрози національній безпеці, що виникають у результаті ворожих інформаційних кампаній. Прикладом практичного застосування є методологія моніторингу стратегічних комунікацій, прийнята Міністерством оборони України, яка використовується для виявлення ризиків дезінформації та пропаганди [25; 35].

- **Міжнародно-нормативний підхід.** Цей підхід ґрунтується на міжнародно визнаних стандартах, таких як ISO/IEC 27005 та NIST SP 800-30, а також на рекомендаціях Організації Об’єднаних Націй, НАТО та Європейського Союзу. Вона дозволяє державам прийняти стандартизовані механізми оцінки ризиків,

що сприяє співпраці з союзниками та міжнародними організаціями. Цей підхід є особливо важливим для координації політики кіберзахисту та реагування на транснаціональні загрози, що відображено в Заяві НАТО про кіберзахист та послідовних звітах Групи урядових експертів ООН (UNGGE) [97; 98].

- **Економіко-вартісний та мотиваційно-евристичний підхід**. Цей підхід враховує інвестиції в інформаційну безпеку та оцінює ризики з точки зору потенційних фінансових втрат. Він базується на таких моделях, як модель Гордона-Лобе, яка оцінює оптимальний рівень інвестицій у кібербезпеку [61], а також на евристичних механізмах, що враховують соціально-психологічні характеристики та мотивацію зловмисних суб'єктів [41]. У міжнародному контексті цей підхід допомагає державам та організаціям оптимізувати витрати на кіберзахист, одночасно максимізуючи ефективність.

- **Моделювання ризиків в умовах невизначеності**. У випадках, коли немає точних даних, але потрібно швидко прийняти рішення, аналіз ризиків спирається на методи моделювання. До них належать моделі нечіткої логіки, багатофакторний аналіз та автоматизовані системи оцінки ризиків [42; 101]. Такі методології є особливо актуальними в контексті гібридних загроз, кібератак та інформаційних операцій, де рівень невизначеності є високим, а масштаби ризику важко передбачити. Застосовуючи моделі невизначеності, держави та організації можуть підвищити свою стійкість та покращити процес прийняття рішень у нестабільних інформаційних середовищах.

Окрім цих методологічних підходів, важливо враховувати міжнародні нормативно-правові рамки та стандарти, що визначають структуровані, систематичні та детальні підходи до управління та зменшення загроз інформаційній безпеці. Ці норми надають теоретичні та практичні рекомендації, що дозволяють організаціям та державам узгодити свої практики з глобальними стандартами управління та управління ризиками.

Стандарт ISO/IEC 27001 встановлює вимоги до системи управління інформаційною безпекою (ISMS), зосереджуючись на підході до захисту конфіденційних даних, що базується на ризиках. Він включає оцінку ризиків, їх обробку, моніторинг та постійне вдосконалення і залишається найбільш визнаною міжнародною сертифікацією в галузі управління інформаційною безпекою. ISO/IEC 27005 доповнює ISO 27001, надаючи детальні вказівки щодо проведення оцінки ризиків та розробки відповідних стратегій їх мінімізації, забезпечуючи детальний, ітеративний процес постійного вдосконалення безпеки (ISO/IEC, 2022) [66; 67; 68].

Національний інститут стандартів і технологій США (NIST) розробив систему кібербезпеки (CSF) та систему управління ризиками (RMF), які містять вичерпні рекомендації щодо виявлення, оцінки та управління ризиками кібербезпеки. CSF NIST визначає п'ять основних функцій — виявлення, захист, виявлення, реагування та відновлення — які відображають безперервний життєвий цикл операцій з безпеки. Система управління ризиками, яка широко використовується у федеральному секторі та секторі оборони, інтегрує безпеку на всіх етапах функціонування системи, акцентуючи увагу на управлінні, підзвітності та постійному моніторингу [75; 76].

FAIR Framework (Факторний аналіз інформаційних ризиків) представляє кількісну модель оцінки інформаційних ризиків шляхом аналізу частоти та впливу потенційних подій. Такий підхід дозволяє особам, що ухвалюють рішення, оцінювати ризики у фінансовому вимірі, що дає змогу визначити пріоритетність ресурсів та провести аналіз витрат і вигод для інвестицій у безпеку. Аналогічно, система COBIT, розроблена ISACA, надає модель управління, яка узгоджує управління IT, кібербезпеку та цілі підприємства. COBIT наголошує на цінності для зацікавлених сторін, структурах управління та стратегічній узгодженості між бізнесом та управлінням IT-ризиками, інтегруючи заходи безпеки в ширшу екосистему корпоративного управління [67].

Одне з нещодавних напрацювань, Норми з управління ризиками штучного інтелекту (AI RMF) Національного інституту стандартів і технологій (NIST), стосується ризиків, пов'язаних із системами штучного інтелекту, включаючи цілісність даних, упередженість і прозорість. Основна увага приділяється чотирьом основним напрямкам — регулюванню, плануванню, вимірюванню та управлінню — які допомагають організаціям розробляти відповідальні, безпечні та зрозумілі системи штучного інтелекту. Ця модель є особливо актуальною для сучасної інформаційної безпеки, де ШІ-системи як створюють, так і зменшують нові категорії ризиків [77].

Разом ці міжнародні нормативні напрацювання утворюють багатошарову систему управління, в якій поєднуються виявлення ризиків, здійснення контролю та постійний моніторинг зі стратегічним наглядом та людськими факторами. Вони сприяють узгодженню глобальних стандартів, пропонуючи універсальну мову для визначення загроз, вразливостей та наслідків у різних секторах і правових системах. Заохочуючи ітеративні процеси, міжгалузеву співпрацю та постійне навчання, ці норми підвищують інституційну та національну стійкість до мінливого ландшафту інформаційних загроз. Їх застосування зміцнює потенціал у сфері кібербезпеки, одночасно сприяючи формуванню культури обізнаності про безпеку, відповідальності та прозорості в глобальній цифровій екосистемі.

Втім, оскільки штучний інтелект продовжує розвиватися, створюючи нові ризики та можливості, надзвичайно важливо приділяти особливу увагу цій сфері. ШІ системи не тільки змінюють існуючі підходи до інформаційної безпеки, але й створюють унікальні вразливі точки, які вимагають окремих структур управління та методологій. Спеціально розроблені для управління інформаційними ризиками, пов'язаними зі ШІ, програми реагують на ці виклики, вирішуючи питання щодо упередженості даних, прозорості та надійності систем, забезпечуючи відповідальний розвиток та впровадження технологій ШІ.

Одна з ключових ініціатив, ISO/IEC JTC 1/SC 42 AI Standards, встановлює міжнародні стандарти управління штучним інтелектом, управління ризиками та етики, а також визначає найкращі практики щодо якості даних, безпеки та оцінки впливу на суспільство [66; 67]. Стандарт IEEE Ethically Aligned Design (Етично узгоджений дизайн) також сприяє інтеграції етичних принципів безпосередньо в розробку систем, тим самим зменшуючи інформаційні та операційні ризики, пов'язані з впровадженням ШІ [62]. Подібно до цього, стандарт ISO/IEC TR 24028:2020 зосереджується на надійності систем ШІ, розглядаючи питання прозорості, доступності пояснень та перевірки результатів роботи ШІ з метою підвищення відповідальності та надійності.

Спеціальні стандарти для штучного інтелекту мають кілька спільних особливостей. Вони стосуються ризиків, характерних для штучного інтелекту, наприклад, алгоритмічної упередженості, відсутності пояснень, конфіденційності даних та відповідальності за автономні рішення. Вони об'єднують міждисциплінарні підходи, що поєднують технічні, етичні та організаційні перспективи, а також заохочують до повторної оцінки ризиків на всіх етапах розробки, впровадження та функціонування штучного інтелекту.

Виходячи зі всього вище зазначеного, це дослідження спирається на сукупність усталених методологічних підходів, включаючи системний, порівняльний, стратегічно-комунікативний та нормативно-правовий аналіз. Ці підходи забезпечують аналітичну основу для виявлення ризиків, оцінки національних та міжнародних заходів реагування, а також вивчення впливу цифрових технологій та штучного інтелекту на глобальну інформаційну безпеку. Доповнення цих методологічних інструментів включенням міжнародних стандартів, таких як ISO, NIST, ENISA, FAIR та COBIT, гарантує, що оцінка ризиків залишається обґрунтованою, структурованою та контекстуально обґрунтованою. З розвитком штучного інтелекту, що несе як ризики, так і можливості, все більшого значення набуває впровадження спеціалізованих

систем, що дозволяють усунути вразливі місця, властиві саме штучному інтелекту.

Разом ці традиційні та ШІ-орієнтовані підходи дозволяють розробляти адаптивні моделі для захисту інформаційних систем і гарантувати, що нові технології зміцнюватимуть, а не підриватимуть глобальне інформаційне поле.

Висновки до розділу 1

Проведений аналіз поняття та еволюції інформаційної безпеки свідчить про те, що вона виросла з вузькотехнічного поняття захисту даних до багатогранної категорії, що охоплює політичні, правові, соціальні та технологічні аспекти. У цифрову епоху інформаційна безпека більше не обмежується лише захистом інформаційних систем, а також стосується забезпечення соціальної стабільності, інституційної довіри та цілісності комунікаційних процесів.

Стрімкий розвиток інформаційних технологій вимагає постійної адаптації систем безпеки до темпів технологічних змін. Тільки шляхом забезпечення своєчасного коригування та координації захисних механізмів держави та організації можуть ефективно знизити ймовірність ризиків, пов'язаних з інформаційними загрозами. У практиці найбільший акцент у розробці систем безпеки робиться на дотриманні нормативних та методологічних рамок, що регулюють захист даних, стійкість мереж та безпеку критичної інфраструктури.

Цифрові технології кардинально змінили сутність інформаційної безпеки. З одного боку, вони сприяють прискоренню обміну знаннями, зростанню цифрової економіки та розширенню глобальних комунікаційних мереж, але з іншого боку, вони створюють безпрецедентні виклики для стабільності інформаційного простору. Зростаючий потенціал штучного інтелекту, машинного навчання та аналізу великих даних розмиває межу між правдою та хибною інформацією, що сприяє підриву довіри до інформаційних систем та інституцій.

Відтак, аналіз ризиків в інформаційній безпеці є важливим процесом, спрямованим на виявлення, оцінку та спостереження за потенційними загрозами, як зловмисними, так і випадковими, та оцінку їхнього впливу на інформаційні системи та дані. Його основною метою є зведення до мінімуму ймовірності втрати інформації або порушення її цілісності. Цей процес включає виявлення ризиків, оцінку ймовірності та потенційного збитку, а також підготовку заходів щодо запобігання або зменшення ризиків, які мають бути інтегровані в ширшу систему управління на організаційному, національному та міжнародному рівнях.

Отже, розвиток інформаційної безпеки відображає більш широкі зміни в парадигмах безпеки в цифрову епоху. Інтеграція системного, порівняльного, стратегічно-комунікативного та нормативно-правового підходів забезпечує концептуальну та аналітичну основу для розуміння цих змін. Доповнення цих методологічних інструментів включенням міжнародних стандартів, а також ШІ-орієнтованих стандартів, дозволяє цілісно розглядати інформаційні ризики як технологічне та соціально-політичне явище, створюючи основу для подальшого розуміння того, як цифрова трансформація змінює майбутнє безпеки у взаємопов'язаному світі.

РОЗДІЛ 2. ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ І ШТУЧНОГО ІНТЕЛЕКТУ НА ГЛОБАЛЬНІ РИЗИКИ

Безпека у сучасному світі формується під впливом складної взаємодії політичних, економічних та технологічних факторів. Серед них цифрові технології, зокрема штучний інтелект (ШІ), є одним із найвпливовіших чинників, що визначають міжнародну інформаційну безпеку. Стрімкий розвиток ШІ, який набуває неймовірної швидкості, змінив процес створення, поширення та споживання інформації. Однак, із появою нових технологій, з'являються і нові ризики. У другому розділі ми розглянемо ключові тенденції, ризики та які статегії застосовують країни задля їх запобігання.

2.1. Ключові технологічні тенденції XXI століття

Темпи технологічного розвитку у XXI столітті є безпрецедентними. Цифрові інновації трансформують політику, економіку, комунікацію, оборону та навіть саму природу міжнародних відносин. Вони не тільки прискорюють потік інформації та розширюють доступ до даних, але й створюють нові вразливі місця в сфері інформаційної безпеки. Як зазначає Юваль Ноа Харарі, сучасні технологічні системи все більше і більше здатні функціонувати автономно, створюючи можливості для інновацій, але водночас становлячи загрозу для демократії, свободи та соціальної справедливості [37]. Діджиталізація суспільства розширила поняття безпеки далеко за межі його традиційного фізичного або військового тлумачення, перетворивши його на багатовимірне явище. Тепер поняття охоплює інформаційні, економічні, політичні, соціальні та екологічні аспекти.

До ключових технологічних тенденцій, що формують сучасний світ, належать штучний інтелект (ШІ) та генеративний ШІ, Інтернет речей (IoT), хмарні та периферійні обчислення, роботизована автоматизація процесів (RPA), блокчейн та досягнення телекомунікації, такі як мережі 5G. Ці новації лежать в основі цифрової економіки та прийняття рішень на основі даних, але вони також

змінюють сферу інформаційної безпеки, створюючи нові вразливі місця та збільшуючи складність управління кіберризиками. Швидке поширення цих технологій розмило межі національної безпеки, оскільки кібератаки та кампанії з дезінформації тепер можна проводити дистанційно та анонімно, що підриває традиційний державний контроль над інформаційними процесами [38; 81].

Серед особливо впливових трендів – стрімкий розвиток штучного інтелекту, зокрема генеративного ШІ. Ці системи здатні створювати величезні обсяги синтетичного контенту – текстового, аудіо- та відео – який може бути використаний для дезінформаційних кампаній та створення фейкових відео [31; 36; 47]. Їхня здатність обробляти величезні масиви даних та виявляти в інших умовах непомітні закономірності значно підвищила оперативну ефективність та посилила механізми раннього попередження в кіберзахисті. Разом з тим, та ж здатність створює вразливі місця, пов'язані із залежністю від даних, непрозорістю алгоритмів та можливістю зловживання з боку супротивників.

Розвиток Інтернету речей (IoT), який з'єднує мільярди пристроїв, від промислових датчиків і транспортних систем до побутової техніки, тісно пов'язаний з цим зростанням. Ефективність та зручність IoT досягаються за рахунок різкого збільшення площі впливу атак. Слабкі стандарти безпеки призводять до того, що критичні інфраструктури, такі як енергетичні мережі або системи охорони здоров'я, стають вразливими до вторгнень, які можуть мати національні або навіть міжнародні наслідки [17; 26]. Уряди стикаються з важким завданням пошуку балансу: хоча економічні вигоди від впровадження IoT є незаперечними, відсутність чітких регуляторних стандартів та уніфікованих систем безпеки збільшує системний ризик.

Завдяки технології блокчейн з'являється децентралізована та захищена від фальсифікацій архітектура даних, яка в свою чергу забезпечує підвищений захист управління ідентифікацією, обміну даними та цілісності транзакцій. Її незмінна структура сприяє прозорості та підзвітності в цифрових взаємодіях і доповнює системи на основі штучного інтелекту, надаючи перевірені дані. Втім,

як і з усіма новітніми розробками, інтеграція цієї технології в критичні інфраструктури створює нові виклики щодо масштабованості, регуляторного нагляду та енергоефективності.

Хмарні та edge-обчислення є ще однією ключовою тенденцією. Ці технології забезпечують масштабоване управління даними та дозволяють створювати додатки з низьким рівнем затримки, такі як автономні транспортні засоби та розумні міста. Водночас саме концентрація конфіденційної інформації на хмарних платформах створює критичні точки вразливості. Порушення безпеки великих хмарних сервісів можуть призвести до одночасного витоку величезних обсягів особистих та інституційних даних, що викликає занепокоєння з приводу цифрового суверенітету та глобальної стійкості [39].

Інша важлива інновація – це впровадження моделі безпеки Zero Trust, яка працює за принципом «ніколи не довіряй, завжди перевіряй». На відміну від традиційних систем захисту на основі периметра, моделі Zero Trust припускають, що загрози можуть існувати як всередині, так і поза мережею. Кожен користувач, пристрій і додаток повинні постійно проходити аутентифікацію та авторизацію доступу, що значно зменшує ймовірність поширення загрози в разі порушення безпеки [59].

Досягнення в галузі автоматизації та роботизованої автоматизації процесів (RPA) також прискорюють робочі процеси та зменшують кількість людських помилок у різних галузях. Однак залежність від автоматизованих процесів може збільшити масштаб збитків у разі їх зловживання. Зловмисне маніпулювання автоматизованими системами може поширити помилки по всій мережі, що робить прозорість, нагляд та стійкість важливими факторами цифрового управління [26; 39; 70; 88].

Телекомунікації, зокрема впровадження мереж 5G, є ще однією революційною трендом. Посилена пропускна здатність 5G підтримує інтеграцію Інтернету речей, штучного інтелекту та інших нових технологій, але водночас

збільшує обсяг і швидкість потоків даних, які можуть бути перехоплені. Більше того, геополітична конкуренція навколо інфраструктури 5G підкреслює її подвійну роль як каталізатора глобальної цифровізації та нового фронту міжнародної конкуренції [72; 74].

Крім того, відбуваються інші структурні трансформації, зокрема поширення дистанційної роботи та розподілених обчислювальних середовищ, що назавжди змінило кордони організацій. Поширення технологій віддаленого доступу, персональних пристроїв та децентралізованих мереж передачі даних вимагає нових підходів до захисту кінцевих користувачів, безпечних протоколів зв'язку та управління ідентифікацією. Водночас інструменти автоматизації та координації оптимізують реагування на інциденти, дозволяючи командам з безпеки ефективніше реагувати на дедалі складніші кіберзагрози.

Варто також зазначити, що розвиток цифрових технологій впливає не лише на технічний, але й на етичний вимір безпеки. Проблеми конфіденційності, приватності, прав доступу та використання даних стають предметом глобальних дискусій і вимагають узгодження на рівні міжнародного права.

В цілому ці тенденції свідчать про докорінну трансформацію парадигми інформаційної безпеки. Ця галузь перетворилася з реактивної та ізольованої дисципліни на інтегровану, інтелектуальну систему безперервного моніторингу, запобігання та адаптації. Передові технології тепер слугують як інструментами захисту, так і джерелами ризику, підкреслюючи подвійну природу цифрової трансформації. У міру зникнення кордонів між кіберпростором та фізичною інфраструктурою підтримання інформаційної безпеки вимагає постійних інновацій, міжнародного співробітництва та інтеграції етичних, технічних і регуляторних підходів, щоб технологічний прогрес зміцнював, а не підривав безпеку людей та інституцій.

2.2. Ризики, пов’язані з використанням штучного інтелекту

Як одна з найбільш трансформаційних технологічних тенденцій XXI століття, штучний інтелект (ШІ), в тому числі GenAI, займає центральне місце у формуванні сучасного технологічного та безпекового дискурсу. Інтеграція штучного інтелекту майже в усі сфери соціальної та економічної діяльності істотно вплинула на способи обробки, інтерпретації та захисту даних. Штучний інтелект підвищує аналітичні можливості, сприяє прийняттю рішень та оптимізує системи кібербезпеки за допомогою автоматизації та прогнозного моделювання. Однак саме ці можливості також створюють і нові вразливі місця.

Штучний інтелект набуває все більш подвійного призначення, удосконалюючи як кіберзахист, так і посилюючи кібератаки. Зловмисники все частіше використовують штучний інтелект для автоматизації та масштабування атак за допомогою адаптивного зловмисного програмного забезпечення, фішингу, що генерується штучним інтелектом, та складання мапи вразливостей у режимі реального часу. Такі системи можуть в автономному режимі навчатися на прикладах захисних реакцій, змінюючи вектори атак так, щоб уникнути їх розпізнання. У результаті швидкість, масштабність та продуманість атак ставлять під загрозу традиційні механізми захисту, розширюючи площину уразливості в критично важливих секторах, включаючи енергетику, фінанси, охорону здоров'я та комунікації [3; 47; 88].

Не менш загрозливими є ризики, що спрямовані безпосередньо на системи ШІ. Зловмисники можуть маніпулювати тренувальними базами даних шляхом їхнього пошкодження, вводити зловмисні команди у великі мовні моделі задля вилучення конфіденційних даних або здійснювати зворотну розробку алгоритмів за допомогою методів інверсії моделей. Такі атаки ставлять під загрозу не тільки точність результатів роботи ШІ, але й цілісність цілих систем, які від них залежать. Слабке управління моделями, неперевірені бази даних і відсутність прозорих ланцюгів постачання посилюють ці вразливості, демонструючи, що системи на основі ШІ є не тільки засобами захисту, але й потенційною небезпечною зброєю [26; 31; 43].

The International AI Safety Report 2025, опублікований урядом Великої Британії, містить детальний огляд основних ризиків, пов'язаних із застосуванням технологій штучного інтелекту. Однією з найактуальніших проблем є зловмисне використання штучного інтелекту. Автоматизаційні можливості штучного інтелекту дозволяють створювати масштабні фішингові кампанії, що дають зловмисникам змогу з безпрецедентною точністю використовувати особисті дані та довіру людей. Генеративні моделі можуть створювати реалістичні підроблені відео, аудіозаписи та зображення — так звані «діпфейки» — які використовуються для маніпуляцій, шантажу та дезінформації. Крім того, використання ШІ в автоматизованих кібератаках становить зростаючу загрозу: алгоритми тепер здатні самостійно виявляти вразливі місця, генерувати зловмисний код та адаптуватися для обходу систем безпеки [63].

Тісно пов'язаним з цим є питання конфіденційності та захисту даних. Сама основа ШІ залежить від доступу до величезних масивів даних, які часто містять конфіденційну або особисту інформацію. Попри те, що такі дані є необхідними для навчання потужних моделей, їх накопичення та обробка створюють значні ризики зловживання, витоку або несанкціонованого доступу. Недостатні механізми захисту можуть призвести до фінансових втрат, шкоди репутації та порушень основних прав, що підкреслює нагальну потребу в надійних регуляторних та етичних гарантіях [85; 86].

Ще один рівень ризику пов'язаний з непередбачуваністю та непрозорістю систем вдосконаленого штучного інтелекту. Багато моделей функціонують як «чорні скриньки», що ускладнює відстеження та розуміння процесів прийняття рішень. Така непрозорість створює умови, за яких системи можуть поводитися непередбачувано або шкідливо. У сферах з високими ризиками, таких як охорона здоров'я, оборона або фінанси, неконтрольована поведінка штучного інтелекту може мати серйозні операційні, етичні та навіть геополітичні наслідки.

По мірі прискорення темпів впровадження штучного інтелекту в економіці та суспільстві з'являються системні вразливості. Зростаюча залежність від автоматизованих систем створює нові точки збою: єдина помилка в програмному забезпеченні, пошкодження даних або алгоритмічна упередженість можуть призвести до ланцюгової реакції у взаємопов'язаних мережах, що потенційно може дестабілізувати цілі сектори. У звіті підкреслюється, що така динаміка сприяє виникненню нової форми «технологічної гонки озброєнь», в якій як зловмисники, так і захисники постійно розробляють і застосовують інструменти ШІ, що ускладнює кібернапади та кіберзахист.

Не менш актуальним викликом є вплив ШІ на цілісність інформації та довіру громадськості. Здатність ШІ генерувати великі обсяги синтетичних медіа — тексту, відео та зображень — сприяє швидкому поширенню дезінформації в глобальному масштабі. Це має глибокі наслідки для виборів, фінансових систем та міжнародних відносин. Підрив довіри громадськості до цифрової інформації та інституцій становить одну з найсерйозніших загроз стабільності демократичних суспільств [47; 84; 88].

Поза цифровою сферою вплив ШІ поширюється на соціально-економічну галузь. Автоматизація змінює ринок праці, замінюючи певні категорії кваліфікованих працівників і водночас створюючи нові посади, що вимагають передових досягнень технічних компетенцій. Ця трансформація приносить як можливості, так і зрушення, порушуючи етичні та правові питання щодо захисту прав працівників, рівності доступу та довгострокової стійкості моделей зайнятості в економіці, що базується на ШІ [43].

Протидія цим багатоаспектним ризикам вимагає комплексного підходу, що поєднує спеціалізовані засоби контролю безпеки ШІ, надійне управління даними, постійну перевірку моделей та міждисциплінарну співпрацю. Системи безпеки потребують вдосконалення з метою забезпечення тестування на стійкість до атак, доступності пояснень та відстежуваності рішень ШІ. Крім того,

співпраця між фахівцями з розробки ШІ, кібербезпеки та політичними діячами має вирішальне значення для створення моделі управління, що забезпечує як інноваційність, так і стійкість. Метою є не обмеження розвитку ШІ, а його інтеграція з більш широкими принципами інформаційної безпеки — захистом цілісності даних, збереженням конфіденційності та підтриманням довіри в умовах все більшої автоматизації світу.

У цьому контексті International AI Safety Report 2025 (Міжнародний звіт з безпечного ШІ) надає рекомендації щодо комплексного переліку заходів для зменшення ризиків, пов'язаних із штучним інтелектом, що мають найбільший пріоритет, наголошуючи на тому, що стабільна безпека штучного інтелекту залежить від співпраці між технічними експертами, установами та міжнародними політичними організаціями [63].

Ключові підходи до цього включають розробку надійних і прозорих систем ШІ з убудованими функціями безпеки, які відповідають принципам демократії, забезпечують доступність для інтерпретації та протистоять ворожим атакам. Прозорість у розробці та функціонуванні також сприяє підзвітності та дозволяє проводити незалежну перевірку. Постійний моніторинг та тестування є необхідними для виявлення непередбачуваної поведінки або вразливостей у режимі реального часу, що і дозволяє швидко вносити оновлення та адаптувати засоби захисту.

Тож ШІ є технологією з подвійною природою, переваги та ризики якої тісно пов'язані між собою. Її трансформаційний потенціал може значно посилити цифрову стійкість, але лише за умови, що держави розроблять адаптивні моделі управління, здатні впоратися з мінливими загрозами. Тому ефективна безпека ШІ залежить від балансу між інноваціями та наглядом, що гарантуватиме, що технологічний прогрес не підірве стабільність та цілісність глобальних інформаційних екосистем.

2.3. Стратегії державного реагування на цифрові виклики

У XXI столітті державна політика у сфері цифрової та інформаційної безпеки стала одним із ключових елементів національної стійкості. Стрімкий розвиток цифрових технологій, зокрема штучного інтелекту, хмарних обчислень та Інтернету речей, створив безпрецедентні можливості для модернізації управління, але водночас — нові ризики для національної безпеки.

Попри те, що встановлені міжнародні механізми та спільні ініціативи закладають основу для протидії ризикам, пов'язаним із ШІ та іншими новітніми технологіями, їхній успіх у кінцевому рахунку залежить від того, наскільки ефективно окремі держави впроваджують ці принципи у своїх системах національної безпеки. Саме національні стратегії є оперативним виміром глобального управління новітніх цифрових технологій, втілюючи широкі міжнародні зобов'язання у практичні механізми запобігання, виявлення та реагування.

Україна є прикладом держави, для якої питання інформаційної безпеки має екзистенційне значення. В умовах триваючої російської агресії держава стала мішенню безпрецедентної кількості кібератак і дезінформаційних кампаній, що виявилися одним із головних інструментів гібридної війни. В умовах постійної боротьби та викликів, Україна розробила комплексну систему кібербезпеки та інформаційної стійкості. Підхід країни відображає не тільки її внутрішні пріоритети у сфері безпеки, але й її внесок у більш розширені міжнародні нормативи, спрямовані на забезпечення стабільності, довіри та відповідальності в часи діджиталізації світу та постійних загроз, які з нього випливають.

Стратегія кібербезпеки України, затверджена Президентом Володимиром Зеленським Указом № 447/2021, окреслює три основні напрямки: стримування, кіберстійкість та взаємодія [35]. Кожен принцип включає конкретні стратегічні цілі, спрямовані на посилення спроможності країни реагувати на сучасні цифрові загрози.

Принцип стримування зосереджений на побудові ефективної національної архітектури кіберзахисту шляхом створення кібервійськ та посилення

можливостей протидії розвідці, саботажу та кібертероризму. Він спрямований на стримування потенційних агресорів шляхом консолідації цифрового суверенітету та національного кіберпотенціалу.

Кіберстійкість підкреслює необхідність постійної готовності та координації між усіма учасниками кібербезпеки. Вона передбачає створення єдиної національної системи управління інцидентами та реформування професійної підготовки та досліджень у сфері кібербезпеки. Стратегія надає пріоритет інноваціям та розвитку кваліфікованої робочої сили для забезпечення готовності до поточних та нових кіберзагроз.

Третій принцип, взаємодія, підкреслює співпрацю між державними установами, приватним сектором та міжнародними партнерами. Україна активно співпрацює з Європейським Союзом, НАТО, Сполученими Штатами та Організацією Об'єднаних Націй з метою обміну передовим досвідом, інформацією про кіберінциденти та розслідування міжнародних кіберзлочинів [15; 78; 100].

Така злагоджена система перетворилася на комплексну національну стратегію кібербезпеки, що відповідає європейським та трансатлантичним стандартам. Оновлена стратегія надає пріоритет стійкості критичної інформаційної інфраструктури, запобіганню кібератакам та шпигунству, а також захисту прав людини в цифровій сфері.

Прийняття Закону України № 4336-IX «Про внесення змін до деяких законодавчих актів щодо кібербезпеки» (2025) модернізувало національну систему кібербезпеки, забезпечивши відповідність Директиві ЄС NIS 2. Закон визначає ролі та обов'язки ключових учасників, посилює координаційну функцію Національного координаційного центру з кібербезпеки (НКЦКБ) та запроваджує єдиний підхід до управління ризиками в секторах критичної інфраструктури.

З технічної точки зору Україна продовжує розширювати свою національну інфраструктуру для моніторингу, виявлення та реагування на кіберінциденти. Це включає в себе сучасні системи аналізу загроз, посилення діяльності CERT-UA в рамках Державної служби спеціального зв'язку та захисту інформації (ДССЗІ) та інтеграцію платформ для повідомлення в режимі реального часу. Паралельно з цим модернізуються програми освіти та сертифікації в галузі кібербезпеки з метою підвищення кваліфікації фахівців [25; 27; 36].

Міжнародне співпраця залишається фундаментальною. Україна підтримує тісні партнерські відносини з ЄС, НАТО, США та іншими міжнародними організаціями. Спільні кібернавчання, участь в ініціативі Cyber Rapid Response Teams (CRRTs) в рамках Постійної структурованої співпраці ЄС (PESCO) та співпраця з приватним сектором посилюють обороноздатність країни (NATO CCDCOE, 2024). Громадські та волонтерські ініціативи, такі як IT-армія України, також стали невід'ємною частиною кібернетичної екосистеми держави [15; 24; 36].

Стратегія кібербезпеки України також чітко визнає гібридний характер сучасних загроз. З огляду на масштабні кібератаки, що надходять з боку росії, Україна зосереджується на швидкому відновленні інформаційних систем, протидії дезінформації та зміцненні цифрового суверенітету. Регулярне виявлення ризиків та налагодження міжвідомчої координації забезпечують можливість критичної інфраструктури продовжувати функціонувати в умовах постійної цифрової агресії.

На противагу цьому, політична структура кібербезпеки Сполученого Королівства, очолювана Національним центром кібербезпеки (NCSC), застосовує цілісний підхід із залученням різних зацікавлених сторін для побудови довгострокової цифрової стійкості. Національна кіберстратегія на 2022-2030 роки окреслює п’ять основних напрямків: зміцнення кіберекосистеми Великої Британії, побудова стійкості, протидія загрозам, прагнення до

досягнення глобального лідерства та розвиток потенціалу на майбутнє [73; 74]. Доповненням до цього є План дій з кіберрозвитку (2023), який має на меті стимулювання інновацій, інвестицій та співпраці в галузі [45; 95].

Головним пріоритетом стратегії Сполученого Королівства є захист критичної національної інфраструктури (КНІ) — таких секторів, як енергетика, охорона здоров'я, фінанси та комунікації — шляхом впровадження розробленого законопроєкту про кібербезпеку та стійкість (CSRB), що має на меті покращити управління ризиками та можливості відновлення. Велика Британія просуває модель «Всесуспільства», в якій кібербезпека інтегрована в організаційне управління, а її основою є звітність керівництва та партнерство між державним і приватним секторами. Такі ініціативи, як Cyber Essentials та Cyber Action Toolkit, підтримують малі та середні підприємства (МСП), надаючи безкоштовні ресурси, навчання та страхові стимули для підвищення базової стійкості [45; 46].

Відданість Великої Британії підготовці підкріплюється національними та галузевими кібернавчаннями, включаючи «червоні команди», тестування на предмет проникнення та симуляції на робочому столі. У цих навчаннях беруть участь урядові агентства, оператори CNI та міжнародні партнери, щоб перевірити потенціал реагування в реальних умовах. Аналіз після інцидентів сприяє циклу постійного вдосконалення, забезпечуючи інституціоналізацію отриманого досвіду в політиці та практиці. [73; 74].

Як Україна, так і Велика Британія усвідомлюють, що міжнародне співробітництво є важливою складовою національної кіберстратегії. Інтеграція України до Рамки співробітництва ЄС-НАТО з кіберзахисту, участь в ініціативі CyberEast+ та співпраця з Центром передового досвіду НАТО з кіберзахисту (CCDCOE) підкреслюють її зростаючу роль у міжнародній кібердипломатії [15; 77; 78]. Аналогічно, участь Великої Британії в обміні розвідданими в рамках «П’яти очей» (Five Eyes), спільних кіберпідрозділах та ініціативах ЄС-НАТО з гібридної стійкості демонструє її залученість до колективної безпеки [77; 79].

Нещодавні кібератаки підкреслюють необхідність такої готовності. У 2024 році Велика Британія повідомила про збільшення кількості атак з використанням ПЗ з вимогою викупу та атак на ланцюги постачання у фінансовому та медичному секторах, що призвело до розширення систем повідомлення про інциденти та протоколів обміну інформацією про загрози [94; 95]. Тим часом Україна продовжує зіштовхуватися з атаками, що фінансуються урядом росії, на свою критичну енергетичну та комунікаційну інфраструктуру, включаючи атаки 2023 року на мережі «Укртелекому» та Міністерства оборони (Україна CERT-UA, 2023) [15; 35; 40]. Хоча умови в обох державах значно відрізняються, вони продемонстрували дієвість державно-приватного партнерства, міжнародної координації та постійної адаптації як ключових факторів стійкості.

Якщо говорити про порівняння, модель України можна охарактеризувати як стійкість в умовах конфлікту, що характеризується гнучкістю, розподіленою обороною та цивільно-військовою координацією. Натомість модель Великої Британії представляє собою інституціоналізоване кіберуправління, засноване на регулюванні, управлінні ризиками та інноваціях. Разом ці підходи вкотре підтверджуть еволюцію національної кібербезпеки від ізольованих заходів оборони до глобальної екосистеми спільної відповідальності.

Окрім підходів, що застосовуються Україною та Великою Британією, варто розглянути ще один європейський приклад, який демонструє, як технологічно розвинена держава бореться з цифровими ризиками. Згідно з Глобальним індексом кібербезпеки 2024 [93], Європа наразі посідає перше місце за рівнем розвиненості кібербезпеки. Згідно з Глобальним індексом кібербезпеки, середній рівень готовності країн Європейського Союзу до кіберзагроз становить 91,2 бала зі 100, що свідчить про системність підходів та розвинену законодавчу базу.

Серед європейських країн-лідерів — Фінляндія, країна, яка є прикладом інтеграції інновацій, стійкості та цифрової довіри в свою національну програму безпеки. Фінська модель відображає більш широкий північний принцип, згідно

з яким технологічний прогрес повинен супроводжуватися етичними та безпечними механізмами управління, особливо в умовах діджиталізації суспільства та впровадження електронних носіїв для аутентифікації особи.

Фінська політика у сфері кібербезпеки ґрунтується на Стратегії кібербезпеки на 2024-2035 роки, прийнятій у жовтні 2024 року, в якій викладено комплексний та спільний підхід до забезпечення національної кіберстійкості. Стратегія інтегрує кібербезпеку в концепцію комплексної безпеки Фінляндії, узгоджуючи цифрову захищеність із політичною, економічною та соціальною стабільністю. Вона була розроблена у відповідь на мінливі глобальні загрози, зокрема війну в Україні, вступ Фінляндії до НАТО та швидку діджиталізацію державних і приватних послуг [44; 51; 71].

Документ окреслює чотири основні стратегічні напрямки: компетентна та інноваційна кібер-екосистема; сильна кіберстійкість суспільства; надійні механізми національного та міжнародного співробітництва; та захищений суверенітет, підкріплений можливостями швидкого реагування. Ці пріоритети реалізуються за допомогою конкретних заходів у всіх секторах, причому кожна гілка влади відповідає за фінансування, моніторинг та звітність щодо заходів з кібербезпеки. Національне управління з кібербезпеки здійснює координацію, а Національний центр кібербезпеки (NCSC-FI) під керівництвом Traficom відповідає за технічну реалізацію та реагування на інциденти на державному рівні.

Фінляндія щорічно інвестує приблизно 300 мільйонів євро в кібербезпеку центральних органів влади, зосереджуючи свої зусилля на навчаннях з готовності, тестуванні систем та підвищенні обізнаності в секторах критичної інфраструктури. У квітні 2025 року країна прийняла Закон про кібербезпеку (124/2025), привівши своє національне законодавство у відповідність до Директиви ЄС NIS2 [65], яка вимагає від критичних операторів управління ризиками, регулярних оцінок та звітності до липня 2025 року. Ця система

посилює відповідальність та стандартизацію у державному та приватному секторах, надаючи особливу підтримку малим та середнім підприємствам (МСП) для посилення їх кіберзахисту.

Також, Фінляндія визнає, що рівень кіберзагроз постійно залишається високим, а з 2022 року все частіше трапляються атаки програм-вимагачів та використання вразливостей систем. Щоб протидіяти цим викликам, уряд зосереджує свої зусилля на безперервному моніторингу в режимі реального часу, міжвідомчому співробітництві, прозорій комунікації про кіберінциденти та спільних навчально-тренувальних заходах. Крім того, Фінляндія активно сприяє міжнародній співпраці в галузі кіберзахисту та гармонізації законодавства через ЄС, НАТО та інші глобальні платформи [57; 71].

Загалом, фінська модель демонструє, що кібербезпека є не лише технічною вимогою, а й фундаментальним аспектом національної безпеки та стабільності суспільства. Інтегруючи правові, організаційні та етичні компоненти, Фінляндія надає перспективний приклад того, як розвинені цифрові економіки можуть збалансувати інновації з безпекою, довірою та стійкістю.

Зрештою, стратегії України, Великої Британії та Фінляндії відображають новий глобальний консенсус: кібербезпека є не лише технологічним викликом, а й стратегічним компонентом національної та міжнародної безпеки. Усі три моделі демонструють спільні риси — міжвідомчу координацію, інституційну сталість, орієнтацію на освіту та міжнародну співпрацю. Водночас різниця у підходах відображає історичний досвід, рівень цифровізації, економічний потенціал і стратегічні виклики кожної країни. Досвід Фінляндії з її орієнтацією на попередження ризиків, британська модель із чітким регуляторним механізмом та українська стратегія з акцентом на стійкість під час війни створюють цінне підґрунтя для вироблення універсальних міжнародних стандартів у сфері кібербезпеки.

Висновки до розділу 2

Штучний інтелект (ШІ), включаючи його генеративні форми (GenAI), є однією з найбільш трансформаційних технологічних тенденцій XXI століття і займає центральне місце у формуванні сучасного технологічного та безпекового дискурсу. Постійне вдосконалення та доступність цих систем піднімають важливі питання щодо зберігання, обробки та захисту даних, ставлячи інформаційну безпеку в центр національної та міжнародної політики.

Проведений аналіз цифрових технологій та їх впливу на глобальні ризики вказує на двоїсту природу прогресу: з одного боку, ці інновації сприяють розвитку, комунікації та ефективності, з іншого – розширюють спектр вразливостей в інформаційному середовищі. Стрімкий розвиток штучного інтелекту, Інтернету речей, хмарних обчислень та аналізу великих даних наражають суспільства на нові гібридні загрози, що поєднують технологічні, інформаційні та психологічні аспекти.

У контексті постійного наростання загроз, пов'язаних із штучним інтелектом та цифровими технологіями, ефективність національних стратегій стає ключовим фактором забезпечення кібербезпеки та цифрової стійкості. Україна є особливо важливим прикладом у цьому контексті. Знаходячись на перетині геополітичної конфронтації та технологічних трансформацій і стикаючись із постійною гібридною агресією з боку росії, Україна розробила всебічний підхід до управління кіберризиками та забезпечення інформаційної безпеки. Її національний підхід ілюструє, як держави можуть адаптуватися до викликів цифрової ери.

Однак варто враховувати й досвід інших країн, адже інформаційні ризики не обмежуються межами однієї держави. Порівняльний аналіз різних національних стратегій дає змогу виявити найефективніші підходи та сприяє формуванню універсальної моделі забезпечення інформаційної безпеки. Стратегія кібербезпеки України формується під впливом геополітичних реалій та гібридної війни, тоді як підхід Великої Британії відображає сформовану

інституційну модель, що ґрунтується на управлінні, законодавстві та бурхливо процвітаючій цифровій економіці. Порівняння цих двох випадків показує, як різні контексти формують відмінні, але взаємодоповнюючі моделі кіберстійкості.

Україна може перейняти досвід Великої Британії в інституціоналізації кібербезпеки, зокрема у розробці чітких правових рамок та довгострокових стратегій нарощування потенціалу. І з іншого боку, Велика Британія може перейняти досвід України в моделі адаптивної стійкості, зокрема в інтеграції механізмів швидкого реагування, добровільних підрозділів кіберзахисту та багаторівневої координації між урядом і приватними структурами під час гібридних загроз. Досвід України у протидії масштабній дезінформації та атакам на інфраструктуру, що фінансуються державою, дає цінні уроки щодо оперативної гнучкості, міжгалузевої комунікації та мобілізації суспільства в умовах високого тиску. Фінлядія, зі свого боку, надає перспективний приклад того, як розвинені цифрові економіки можуть збалансувати інновації з безпекою, довірою та стійкістю.

З порівняльного аналізу випливає, що різні країни сьогодні застосовують різні, власні підходи до забезпечення цифрової безпеки та управління штучним інтелектом, що відображає різноманіття політичних систем, рівнів технологічного розвитку та стратегічних пріоритетів. Це різноманіття підходів створює сприятливі умови для міжнародного діалогу, обміну досвідом і спільного вироблення стандартів, які допомагають формувати більш узгоджену глобальну систему реагування на цифрові виклики. Усунення сьогоднішніх викликів, пов’язаних з технологічними тенденціями, вимагає скоординованих міжнародних зусиль, постійного моніторингу та надійних нормативно-правових рамок, що поєднують технологічні запобіжні заходи з етичним і правовим наглядом.

Лише через відповідальне управління технологіями та тісну співпрацю між державами, міжнародними організаціями й приватним сектором можна досягти стійкої рівноваги між технологічним прогресом та інформаційною безпекою, забезпечуючи, щоб інновації зміцнювали, а не підривали глобальну стабільність.

РОЗДІЛ 3. МІЖНАРОДНА СПІВПРАЦЯ У ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

Незважаючи на те, що Україна продовжує реалізовувати власні стратегії ефективного протидії цифровим ризикам, не менш важливо розглядати ці ініціативи в глобальному контексті та аналізувати, як міжнародні партнери України вирішують проблеми, пов’язані з новітніми цифровими технологіями. У цьому розділі розглядається роль кібердипломатії, ініціативи міжнародних організацій та перспективи, що формують глобальну реакцію на цифрові загрози в контексті інформаційної безпеки.

3.1. Роль кібердипломатії у забезпеченні інформаційної безпеки

Кібердипломатія стала одним з найважливіших інструментів сучасних міжнародних відносин, що відображає трансформацію глобальних пріоритетів безпеки в епоху цифрових технологій. У міру того як інформаційні системи, комунікаційні мережі та штучний інтелект стають центральними елементами функціонування держави, дипломатія все більше поширюється на кіберпростір, вирішуючи питання, що виходять за межі кордонів і вимагають постійної багатосторонньої взаємодії. Перехід від традиційної дипломатії до кібердипломатії свідчить про усвідомлення того, що цифровим загрозам — включаючи кібератаки, дезінформаційні кампанії, гібридні операції та маніпуляції за допомогою штучного інтелекту — не можна протистояти виключно на державному рівні.

Кібердипломатія передбачає використання дипломатичних механізмів для досягнення цілей у сфері кібербезпеки — від узгодження міжнародних правил і стандартів до координації відповідей на кібератаки, а також розбудови довіри між державами. Її роль стрімко зростає, оскільки цифрові загрози дедалі частіше мають транскордонний характер і не обмежуються юрисдикцією окремих країн. Формування глобальної архітектури кібербезпеки, у межах якої держави взаємодіють на основі принципів прозорості, відповідальності та взаємної довіри, стає одним із головних завдань міжнародного порядку денного.

Ключові функції кібердипломатії можна розглядати в декількох взаємопов'язаних площинах. По-перше, вона сприяє формуванню міжнародних норм і правил у кіберпросторі. За допомогою дипломатичних переговорів держави координують стандарти належної етики поведінки, що допомагає запобігти ескалації кіберконфліктів і зменшити ймовірність кібервійни. По-друге, кібердипломатія сприяє встановленню та підтримці міжнародних партнерських відносин, що дає країнам можливість обмінюватися інформацією про кіберзагрози, координувати реагування на кіберінциденти та проводити спільні розслідування кіберзлочинів. Третя функція — боротьба з кіберзлочинністю та кібертероризмом, де дипломатичні механізми слугують платформами для співпраці в галузі правоохоронної діяльності, обміну інформацією та нарощування потенціалу для протидії транснаціональним загрозам. Зрештою, кібердипломатія підтримує захист національних інтересів, допомагаючи державам просувати свої зовнішньополітичні цілі, захищати критичну інфраструктуру та особисті дані, а також виступати за етичне та правове регулювання нових технологій [29].

Зростаюча складність цифрових загроз підкреслює необхідність всебічного та безперервного міждержавного діалогу. Такі питання, як все більш широке використання штучного інтелекту в кібератаках, масштабні кампанії з дезінформації та гібридні операції, вимагають гнучких дипломатичних відповідей. Роль дипломатів у цій сфері виходить за межі традиційних переговорів — зараз вони беруть участь у розробці політики, реагуванні на кризи та розробці міжнародних кібернорм. Підтримка кіберкомпетентності в дипломатичних установах стала необхідною умовою для реалізації ефективної глобальної політики у сфері кібербезпеки [12; 52].

Таким чином, кібердипломатія є основою сучасної системи інформаційної безпеки. Саме вона дозволяє державам діяти спільно в глобальному цифровому середовищі, зберігаючи при цьому баланс між безпекою, правами людини та індивідуальними свободами.

Україна на практиці демонструє низку успішних прикладів кібердипломатії. Одним із таких прикладів є поглиблення співпраці з Європейським Союзом та НАТО. Україна активно інтегрується в західні структури кібербезпеки, бере участь у кібердіалогах та ділиться своїм унікальним досвідом протидії російській кіберагресії. Під час третього раунду кібердіалогу між ЄС та Україною обидві сторони домовилися про посилення співпраці, а українська делегація надала стратегічні рекомендації на основі національної практики забезпечення стійкості [15, с.30].

Ще один приклад – двостороння співпраця зі Сполученими Штатами, яка включає обмін знаннями та спільні ініціативи, такі як «Кіберміст США–Україна» та участь у серії конференцій «Hack the Capitol». Українські експерти з кібербезпеки на регулярній основі діляться своїм досвідом у сфері цифрової оборони, а американські партнери та ІТ-коаліції надають технічну допомогу, ліцензії на програмне забезпечення та обладнання для вдосконалення кіберінфраструктури України [15, с.31; 100].

На додаток до цього, Україна запровадила національні стратегії та плани дій у сфері кібердипломатії. У 2023 році Міністерство закордонних справ України представило план інтеграції кібердипломатії в більш широку діяльність у сфері зовнішньої політики. Це включає створення спеціальних каналів комунікації з міжнародними партнерами, впровадження кіберполітики в дипломатичні місії та посилення співпраці з регіональними організаціями та альянсами [23; 35].

Вступ України до Центру передового досвіду НАТО з питань кіберзахисту (CCDCOE) у Таллінні в 2023 році стало ще однією сходинкою у зміцненні міжнародного кіберспівробітництва [78]. Цей крок розширив доступ України до спільних розвідданих, навчання та механізмів колективного реагування, що є частиною ширшої міжнародної коаліції з кіберзахисту [77; 87].

Україна є прикладом цифрової дипломатії завдяки глобальному просуванню своїх інновацій у сфері електронного урядування. Міжнародне поширення української платформи « Diia » та її ініціатив у сфері цифрової ідентифікації є прикладом того, як цифрові рішення можуть сприяти прозорості та стійкості урядування, стаючи інструментом м'якої сили у зовнішній політиці [25; 27; 35].

Для порівняння, стратегія кібердипломатії Сполученого Королівства є частиною більш широкої Національної кіберстратегії та програми цифрової зовнішньої політики, спрямованої на позиціонування Великобританії як світового лідера у просуванні відповідального та демократичного цифрового врядування. Підхід Великої Британії побудований навколо кількох стратегічних напрямків: міжнародне співробітництво, регуляторна та нормотворча роль, розбудова кіберпотенціалу, просування демократичних цифрових цінностей та інтеграція кібердипломатії з внутрішніми пріоритетами, такими як захист критичної інфраструктури та управління штучним інтелектом [45; 46; 73; 74; 94].

Завдяки своєму головуючому статусу в НАТО, G7, ООН та Співдружності, Велика Британія бере участь у формуванні міжнародних кібернорм та правил діяльності в кіберпросторі. Вона сприяє розвитку систем регулювання штучного інтелекту, захисту даних та цифрової торгівлі, забезпечуючи їх відповідність правам людини та демократичним цінностям (Парламент Великої Британії, 2023). Велика Британія також активно сприяє розбудові кіберпотенціалу держав-партнерів, особливо в регіонах, що розвиваються, шляхом надання навчання, консультативної підтримки та ініціатив з передачі знань [73; 74].

У рамках НАТО Велика Британія відіграє ключову роль в оперативній координації та стратегічній комунікації. Вона сприяє реалізації політики НАТО у сфері кіберзахисту, бере участь у спільних навчаннях, таких як Cyber Coalition та Locked Shields, а також сприяє обміну інформацією через CCDCOE [77; 79]. Така залученість забезпечує Великій Британії провідну роль у

багатонаціональній готовності, а також зміцнює взаємодію та здатність до спротиву в рамках альянсу.

З порівняльної точки зору, українська кібердипломатія відображає модель стійкості через інтеграцію, де активна співпраця та участь у міжнародних альянсах слугують як оборонною необхідністю, так і дипломатичним інструментом для світового визнання. На відміну від цього, модель Великої Британії втілює стратегічне лідерство, використовуючи свою усталену дипломатичну мережу, нормативно-правовий вплив та технологічний досвід для формування міжнародних цифрових норм.

Незважаючи на ці відмінності, обидві країни розділяють прихильність до багатосторонніх відносин та спільної відповідальності у кіберпросторі. Досвід України в умовах гібридного конфлікту дає практичні уявлення про кризову дипломатію та зміцнення стійкості, які можуть бути корисними для політики Великої Британії та НАТО щодо швидкого реагування та адаптивного управління. І навпаки, інституційний досвід Великої Британії в галузі кіберрегулювання, нормативних рамок та управління штучним інтелектом надає Україні моделі для консолідації її післявоєнної цифрової трансформації в європейському та трансатлантичному контексті.

Спільними зусиллями Велика Британія та Україна демонструють два взаємодоповнюючих шляхи зміцнення глобальної кібердипломатії: один ґрунтується на стратегічному передбаченні та нормативному лідерстві, інший — на адаптивній співпраці та оперативній стійкості. Їхня діяльність підкреслює еволюцію ролі дипломатії в цифрову епоху, коли забезпечення безпеки інформаційного простору залежить не тільки від технологій, а й від альянсів та спільного управління.

У перспективі посилення двосторонньої кібердипломатії між Великою Британією та Україною може стати зразком для майбутніх трансатлантичних цифрових партнерств. Посилення співпраці в таких сферах, як управління

штучним інтелектом, освіта в галузі кібербезпеки, спільні тренінги з питань стійкості та координація реагування на кризові ситуації, дозволить обом країнам поєднати регуляторний та інституційний досвід Великої Британії з практичним досвідом України в галузі управління кіберконфліктами. Шляхом поглиблення стратегічної координації та обміну знаннями обидві країни зможуть спільно сприяти формуванню більш безпечного, прозорого та стійкого глобального цифрового середовища, в якому інновації досягаються не за рахунок безпеки, а у поєднанні з нею.

Можна зазначити, що кібердипломатія виступає каталізатором міжнародної співпраці у сфері інформаційної безпеки, тим самим сприяючи узгодженню правових рамок, обміну досвідом і підвищенню стійкості держав до глобальних цифрових викликів. Вона не просто реагує на загрози. Нині кібердипломатія створює платформу для формування нового світового порядку, у якому безпека, новітні технології та права людини взаємодіють на основі спільної відповідальності.

3.2. Міжнародні ініціативи та багатосторонні формати співпраці

Сучасна система міжнародної інформаційної безпеки формується на перетині технологічного розвитку, політичних рішень і правових механізмів. У глобалізованому цифровому середовищі жодна держава не здатна самостійно гарантувати захист від кіберзагроз, тому міжнародне співробітництво стає центральним чинником ефективного реагування на виклики. Спільні ініціативи, багатосторонні формати та міжнародні угоди створюють основу для узгоджених дій держав, спрямованих на зміцнення стійкості кіберпростору, розробку універсальних стандартів безпеки та підтримку довіри у міжнародних відносинах.

Тому для сфери інформаційної безпеки характерний широкий спектр міжнародних ініціатив та багатосторонніх механізмів співпраці, спрямованих на протидію кіберзагрозам, обмін досвідом та розробку спільних стандартів

безпеки. Ці кроки свідчать про зростаюче усвідомлення того, що проблеми кібербезпеки мають транснаціональний характер і вимагають колективних глобальних заходів реагування [27].

Серед основних міжнародних ініціатив Організація Об'єднаних Націй (ООН) відіграє фундаментальну роль у формуванні правової та інституційної бази для глобального співробітництва. Через свої спеціалізовані агентства та резолюції ООН сприяє встановленню міжнародних норм відповідальної поведінки держав у кіберпросторі та організовує спеціальні форуми, експертні групи та семінари, присвячені безпеці інформаційно-комунікаційних технологій (ІКТ). Зокрема, Робоча група ООН відкритого складу (OEWG) та Група урядових експертів (GGE) досягли прогресу у діалозі щодо застосування міжнародного права в кіберпросторі [22; 97; 98; 99].

Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (IEC) сприяють глобальному управлінню кібербезпекою через свої стандарти, зокрема ISO/IEC 27001, який встановлює міжнародні вимоги до систем управління інформаційною безпекою. Ці ж стандарти надають єдину основу для оцінки та управління кіберризиками в різних секторах та юрисдикціях [30].

Міжнародна спілка електрозв'язку (МСЕ), що є спеціалізованою установою ООН, відіграє важливу роль у координації глобальних зусиль, покликаних посилити кібербезпеку та захистити інформаційні та комунікаційні мережі. МСЕ розробляє технічні рекомендації, просуває передові практики та сприяє нарощуванню потенціалу через такі ініціативи, як Глобальний індекс кібербезпеки (GCI), який визначає рівень кіберготовності держав-членів [64].

Серед інших останніх ініціатив – Глобальна угода про безпечний розвиток штучного інтелекту, яка об'єднує 27 країн, включаючи Європейський Союз та Україну. Ця ініціатива спрямована на встановлення скоординованих міжнародних принципів етичного та безпечного просування технологій

штучного інтелекту з метою запобігання зловживанням та системним ризикам [34].

Багатосторонні формати співпраці є не менш важливими для зміцнення стійкості та спільної відповідальності. Організація Північноатлантичного договору (НАТО) та Європейський Союз (ЄС) є головними ініціаторами таких зусиль. Обидві організації проводять спільні кібернавчання, обмінюються розвідданими про кіберзагрози та узгоджують розробку політики з метою посилення колективних оборонних можливостей. Стратегія ЄС з кібербезпеки на цифрове десятиліття та діяльність Агентства Європейського Союзу з кібербезпеки (ENISA) зосереджені на підвищенні кіберстійкості за допомогою регуляторних заходів, оперативних центрів та механізмів транскордонного реагування [30; 53; 54; 55; 56; 58].

Натомість об'єднання БРІКС (Бразилія, росія, Індія, Китай, Південна Африка) та Шанхайська організація співробітництва (ШОС) представляють альтернативні регіональні моделі управління кібербезпекою. Вони сприяють суверенітету держав у кіберпросторі та координують підходи до боротьби з кіберзлочинністю та інформаційною війною [60].

Організація економічного співробітництва та розвитку (ОЕСР) та Азіатсько-Тихоокеанське економічне співробітництво (АТЕС) є досить впливовими платформами для розробки політичних рішень та обміну знаннями. Вони заохочують міжнародний діалог щодо безпеки цифрової економіки, сприяють впровадженню найкращих практик захисту даних та забезпечують підтримку держав-членів у створенні надійних систем кібербезпеки.

Двосторонні та багатосторонні відносини між країнами також передбачають партнерство у сфері кібербезпеки на основі підписання угод, меморандумів та проведення навчальних програм. Україна підписала угоди про партнерство у сфері кібербезпеки з Європейським Союзом, Канадою та іншими

партнерами, зокрема щодо обміну інформацією, спільного розвитку потенціалу та підвищення національної кіберстійкості [33].

Серед типових форм міжнародної співпраці – спільні навчальні заходи, розробка спільних стандартів і рекомендацій у сфері кібербезпеки, розробка скоординованих стратегій реагування на інциденти та прийняття відповідних конвенцій, резолюцій і меморандумів про взаєморозуміння. Ці ініціативи сприяють уніфікації стандартів, ефективному запобіганню глобальним кіберзагрозам та зміцненню інформаційної безпеки в усьому світі [79; 82; 83].

Будапештська конвенція про кіберзлочинність (2001) залишається фундаментом міжнародного співробітництва у боротьбі з кіберзлочинністю, оскільки встановлює правові стандарти для розслідування, судового переслідування та обміну інформацією [50]. В ЄС управління кібербезпекою додатково підтримується Директивою NIS 2, Регламентом ENISA та програмами, такими як CyberEast+, які надають технічну допомогу та навчання країнам-партнерам, зокрема Україні [4; 15; с. 14, 54; 55].

Загалом, міжнародні ініціативи в галузі кібербезпеки мають різний масштаб, пріоритети та механізми, проте разом вони утворюють багаторівневу глобальну архітектуру. Глобальні механізми спрямовані на уніфікацію принципів і стандартів, тоді як регіональні та двосторонні партнерства зосереджуються на впровадженні, підзвітності та оперативній координації. Ця багаторівнева система дає змогу державам будувати комплексні архітектури кібербезпеки та зберігати опір до новітніх глобальних загроз [36].

Для України участь у цих ініціативах сприяє посиленню її спроможності протидіяти гібридним загрозам, адаптувати своє законодавство до міжнародних стандартів та брати участь у глобальних діалогах щодо ефективної державної політики у кіберпросторі. Взаємодія між національними та міжнародними структурами створює взаємопідсилюючу систему, в якій Україна як сприяє колективній безпеці, так і отримує від неї вигоди. У цьому сенсі глобальна

співпраця є важливим доповненням до власної стратегії України у сфері кібербезпеки, що дозволяє країні залишатися активним та впливовим учасником у формуванні міжнародної політики у сфері інформаційної безпеки.

Усі зазначені вище ініціативи свідчать про поступовий перехід від фрагментарного реагування на інциденти до системного міжнародного управління кіберпростором. Міжнародна співпраця дедалі більше охоплює міждержавні формати партнерства, регіональні програми технічної допомоги та академічно-наукові проєкти, спрямовані на створення єдиних стандартів безпеки. Важливо, що у сучасних умовах глобальної нестабільності цифрова безпека стає не лише технічним чи політичним питанням, а частиною ширшої концепції "інформаційного миру", де і дипломатія, і технології, і право взаємодіють задля спільного захисту цінностей людства.

Таким чином, міжнародні ініціативи і багатосторонні формати співпраці створюють складну, але взаємопов'язану архітектуру глобальної кібербезпеки. Їхня ефективність залежить від постійного оновлення механізмів взаємодії, зміцнення довіри між державами та вироблення єдиних стандартів, які дозволяють поєднувати технологічний розвиток із гарантіями прав людини і міжнародного миру.

3.3. Перспективи глобального нормативного консенсусу у сфері цифрових технологій

Сьогоднішній світ стоїть на межі нового етапу формування міжнародного правопорядку — цифрового, де регулювання технологій, даних і штучного інтелекту стає ключовою умовою стабільності. Розвиток цифрових інновацій створює не лише технічні, а й нормативні виклики, оскільки глобальне суспільство має узгодити принципи, за якими розвиватимуться технології, що дедалі більше впливають на політичні процеси, економіку, приватність і навіть безпеку людини.

Перспективи досягнення глобального нормативного консенсусу в галузі цифрових технологій є досить складними та багатогранними. Простежується загальна тенденція до розробки універсальних принципів та прав людини як основи цифрового врядування, проте через розбіжності в інтересах держав, міжнародних корпорацій та громадськості все ще існують суттєві обмеження.

До найбільш значних досягнень належить прийняття Глобального цифрового пакту — додатка до Пакту ООН про майбутнє (Резолюція Генеральної Асамблеї ООН № 79/1 від 22 вересня 2024 року). Саме цей документ є важливим першим кроком до створення спільної основи для міжнародного регулювання у цифровій сфері, зокрема щодо штучного інтелекту. Водночас міжнародні стандарти, такі як ISO/IEC 27001 та пов'язані з ними рамки ISO, отримали світове визнання як інструменти «м'якого права», що все частіше застосовуються в різних правових системах як основа для забезпечення цифрової та інформаційної безпеки [22; 28; 66; 68].

Суттєвою зміною є посилення інтеграції гібридних підходів до регулювання, що поєднують елементи «жорсткого права» (юридично обов'язкові норми) з «м'яким правом» (рекомендації, стандарти та добровільні зобов'язання). Ці підходи залучають широке коло зацікавлених сторін, включаючи уряди, суб'єкти приватного сектору та міжнародні організації, до формування моделей цифрового управління на основі консенсусу.

Однак зберігається низка значних викликів і обмежень. Багатополярний характер політичного та економічного середовища означає, що великі світові лідери, такі як Сполучені Штати, Китай та Європейський Союз, продовжують просувати різні цифрові моделі, що відображають їхні відповідні цінності та інтереси [7; 14]. Наприклад, ЄС виступає за Загальний регламент про захист даних (GDPR) [48; 49] як глобальний стандарт захисту даних, тоді як Китай досягає концепцію «кіберсуверенітету». Крім того, вплив великих технологічних корпорацій та суперечливі пріоритети щодо ринків даних, конфіденційності та

безпеки перешкоджають встановленню єдиних глобальних стандартів. Відсутність ефективних механізмів виконання міжнародних угод, навіть тих, що прийняті на основі консенсусу (таких як Глобальний цифровий пакт), ще більше ускладнює прогрес у напрямку прийняття обов'язкових нормативних актів.

У довгостроковій перспективі зростає ймовірність того, що взаємне визнання стандартів м'якого права стане основним інструментом для узгодження національних регуляторних режимів. У середньостроковій перспективі очікується досягнення консенсусу шляхом поступової згоди щодо універсальних стандартів, а не за допомогою жорстких правових інструментів. Цей процес, ймовірно, буде сприяти багатосторонньому діалогу та поступовому узгодженню внутрішнього законодавства. Права людини, прозорість, інклюзивність та підзвітність дедалі більше вбудовуються в основу глобальних ініціатив, навіть за відсутності обов'язкового виконання. Ці принципи становлять основу для потенційної майбутньої структури глобального цифрового врядування.

Водночас нові виклики — зокрема, зростання потужності генеративних моделей, автоматизація рішень у сфері безпеки, посилення дезінформаційних кампаній — потребують не лише нормативних, а й технологічних гарантій безпеки. Тому майбутній консенсус має передбачати інтеграцію міжнародного права з технічними стандартами, забезпечення прозорості алгоритмів, контроль за використанням військового штучного інтелекту та підтримку відкритих наукових досліджень.

Висновки до розділу 3

Вивчення міжнародного співробітництва та кібердипломатії підтверджує, що інформаційна безпека в цифрову епоху не може бути досягнута за допомогою виключно національних зусиль. Вона залежить від скоординованих багатосторонніх дій, які об'єднують держави, міжнародні організації та інших учасників у розробці спільних принципів та превентивних механізмів.

Ряд ініціатив наочно ілюструє процес зміцнення інституціоналізації глобальної співпраці в інформаційній сфері. Організація Об'єднаних Націй створила такі структури, як Робоча група відкритого складу (OEWG) та Група урядових експертів (GGE), які слугують ключовими платформами для діалогу та розробки норм у кіберпросторі. Будапештська конвенція про кіберзлочинність залишається основоположним міжнародним інструментом боротьби з кіберзлочинами, забезпечуючи правову базу для транскордонної співпраці й обміну цифровими доказами. Зобов'язання НАТО щодо кіберзахисту та ініціативи, такі як CyberEast+, ще раз ілюструють зростаючий акцент на спільній готовності та нарощуванні потенціалу в країнах-партнерах.

Сучасна кібердипломатія знаходиться на стику технологій, безпеки та міжнародних відносин, тим самим відображаючи зростаючу взаємозалежність між цифровою трансформацією та глобальною стабільністю. Зважаючи на те, що інформаційні загрози виходять за межі національних кордонів, здатність держав співпрацювати, домовлятися про спільні норми та зміцнювати довіру в кіберпросторі визначає їхню колективну стійкість. Досвід України та Великої Британії ілюструє дві різні, але схожі моделі цього процесу — одна сформована конфліктом та необхідністю термінової адаптації, інша — довгостроковою стратегією та інституційним передбаченням.

Для України кібердипломатія стала важливим інструментом національного захисту та міжнародної інтеграції. Зіткнувшись із постійною гібридною війною та масштабною кіберагресією з боку росії, Україна використовує дипломатію для зміцнення своєї стійкості шляхом взаємодії з ЄС, НАТО та іншими партнерами. Її приєднання до Центру передового досвіду НАТО з питань кіберзахисту, участь у робочих групах ООН з відкритим складом та лідерство в рамках кібердіалогу між ЄС та Україною підкреслюють її перетворення з отримувача кібердопомоги на проактивного учасника міжнародного діалогу з питань безпеки. Таким чином, підхід України до кібердипломатії не обмежується лише обороною. Кібердипломатична стратегія

України - це також засіб утвердження цифрового суверенітету, зміцнення міжнародної легітимності та позиціонування себе як регіонального лідера у сфері розбудови кіберпотенціалу.

У цілому, розвиток механізмів міжнародного співробітництва відображає визнання того, що інформаційна безпека є спільною відповідальністю та ключовим елементом глобальної стабільності. Реалізація таких ініціатив, які здійснюються під егідою ООН, ЄС та НАТО, демонструє потенціал скоординованих дій для зміцнення довіри, запобігання ескалації конфліктів та підвищення стійкості у цифровій сфері. Постійне залучення інвестицій у ці механізми співробітництва є надзвичайно важливим для підтримання миру, безпеки та прозорості у глобальному інформаційному просторі.

ЗАГАЛЬНІ ВИСНОВКИ

Цифрова трансформація XXI століття суттєво змінила параметри міжнародної безпеки, створивши нові можливості для розвитку і одночасно загострившись глобальні ризики. Інформація перетворилась із допоміжного інструменту управління на стратегічний ресурс, що тепер визначає політичну, економічну та соціальну стабільність. У даному контексті інформаційна безпека вийшла за межі традиційних технічних обмежень і стала міждисциплінарною галуззю, що охоплює право, етику, міжнародні відносини та регулювання технологіями.

Проведене дослідження свідчить про те, що інформаційна безпека зазнала парадигмальних змін. Вона більше не обмежується захистом даних, а представляє собою системний процес підтримання цілісності, доступності та конфіденційності інформації в складних соціально-технічних системах. Цифрова революція змінила не лише механізми захисту, а й саму природу загроз та вразливостей.

Постійний розвиток таких технологій, як штучний інтелект, Інтернет речей, аналіз великих даних та хмарні обчислення, змінює межі інформаційного простору. Ці інструменти забезпечують швидкі інновації та зростання, але водночас створюють безпрецедентні загрози. Ті самі алгоритми, що покращують процес прийняття рішень та комунікацію, можуть бути використані як зброя для маніпулювання суспільною думкою, підриву інфраструктури або порушення демократичних процесів.

Для аналізу цих процесів необхідний мультидисциплінарний та адаптивний підхід. Ефективне управління інформаційною безпекою залежить від уміння виявляти ризики, оцінювати їхній потенційний вплив та інтегрувати запобіжні заходи в більш широкі системи управління. Методи, що поєднують системний, порівняльний та нормативно-правовий виміри, надають необхідні концептуальні інструменти для розуміння інформаційної безпеки не лише як

оборонного механізму, а й як соціальної та політичної інституції, що постійно розвивається. У цьому сенсі аналіз ризиків стає як технічним, так і стратегічним завданням, яке вимагає постійного перегляду у міру розвитку технологій.

Український досвід є наочним прикладом того, як держава може адаптуватися до викликів цифрової безпеки в умовах гібридної війни. Національна стратегія кібербезпеки України демонструє, що стримування, стійкість та міжнародне співробітництво утворюють детальну систему реагування на військові та невійськові загрози в кіберпросторі. Цей приклад не тільки підкреслює необхідність національної готовності, але й показує цінність міжнародних партнерств для зміцнення цифрової оборони та захисту критичної інфраструктури.

Міжнародний контекст підтверджує, що інформаційну безпеку неможливо забезпечити за допомогою виключно внутрішніх заходів. Створення механізмів співпраці під егідою Організації Об'єднаних Націй, Європейського Союзу, НАТО та інших інституцій відображає зростаюче усвідомлення того, що кіберзагрози мають глобальний характер. Такі ініціативи, як Будапештська конвенція про кіберзлочинність, Директива ЄС NIS 2 та Кіберзахисна політика НАТО, свідчать про реальний прогрес у напрямку створення спільних стандартів та взаємної підтримки. Кібердипломатія слугує сполучною ланкою цієї структури — вона сприяє діалогу, зміцненню довіри та спільній реакції на події, з якими будь-яка держава не змогла б впоратися самостійно.

Попри це, залишаються значні виклики. Розбіжності в національних інтересах, асиметрія в технологічних можливостях та відсутність загальноприйнятих правових норм ускладнюють зусилля з побудови єдиної глобальної системи кібербезпеки. Крім того, вплив транснаціональних корпорацій та неурядових організацій ще більше розмиває межі відповідальності. Ці перепони підкреслюють важливість продовження

дипломатичного діалогу та розробки гнучких механізмів, що забезпечують баланс між незалежністю та взаємозалежністю.

У більш широкому сенсі, результати цього дослідження вказують на фундаментальну істину: інформаційна безпека є сьогодні показником суверенітету, легітимності та довіри. Її захист не може бути досягнутий виключно за допомогою технологій. Окрім цього, він вимагає колективної відповідальності, етичних зобов'язань та дипломатичного співробітництва. Інтеграція штучного інтелекту та постіний розвиток новітніх технологій в усі аспекти соціального та політичного життя вимагає нового підходу до підзвітності, прозорості та інклюзивності в управлінні.

У перспективі можна окреслити кілька напрямків досліджень і політики. По-перше, виникає необхідність продовжувати порівняльний аналіз стратегій окремих держав у сфері кібербезпеки та управління штучним інтелектом, щоб визначити найкращі практики збалансування інновацій та зменшення ризиків. По-друге, слід посилити міждисциплінарні дослідження, що поєднують інформатику, право, міжнародні відносини та етику для того, щоб розробити адаптивні рамки для нових технологій, таких як квантові обчислення та генеративний штучний інтелект. По-третє, більшу увагу слід приділяти створенню систем безпеки, орієнтованих на людину, а саме таких, що не тільки захищають дані, але й розширюють можливості окремих осіб, зберігають демократичні цінності та зміцнюють соціальну довіру в цифровій сфері.

З переходом до цифрового світу, інформаційна безпека постала одночасно спільним викликом і колективною відповідальністю. Як показує досвід України та Великої Британії, для забезпечення безпеки в цифрову епоху потрібно не тільки працювати у сфері захисту, а й співпрацювати, передбачати та керувати, спираючись на етику і верховенство права. Завдяки відповідальним інноваціям, інклюзивній дипломатії та етичному регулюванню міжнародна спільнота може

перетворити цифрову вразливість на можливість для стабільності та довіри у світовому інформаційному середовищі.

У практичному плані, висновки, отримані в результаті цього дослідження, можуть допомогти державним діячам, науковцям та практикам у вдосконаленні стратегій управління кібербезпекою. Шляхом аналізу існуючих технологічних тенденцій та визначення найактуальніших ризиків, дослідження надає концептуальну основу для розробки превентивних та адаптивних заходів політики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади. Дис. … д-ра юрид. наук: 12.00.07. Харків: Нац. ін-т внутр. справ, 2002. 408 с.
2. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю // *Mind.ua*. — 24 квітня 2024 р. — [Електронний ресурс]. — Режим доступу: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu (дата звернення: 18.10.2025).
3. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Інститут проблем політики та інформаційного суспільства. URL: https://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya-“kiberbezpeka” (дата звернення: 18.10.2025).
4. Бєляков К. І. Внутрішня безпека України і шляхи її забезпечення. Київ: МНДЦ, 2005. С. 26–32.
5. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Mechanism of Economic Regulation. 2014.
6. Бостром Н. Суперінтелект. Стратегії і небезпеки розвитку розумних машин. Київ: Наш формат, 2020. 408 с.
7. Вебб Е. Велика дев’ятка. Як IT-гіганти та їхні розумні машини можуть змінити людство. Харків: Vivat, 2020. 352 с.
8. Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам. С. 105–110.
9. Гаврильців М. Т. Інформаційна безпека держави у системі національної безпеки України. Юридичний науковий електронний журнал. 2020.
10. Гіґґінз Е. Ми – Bellingcat. Онлайн-розслідування міжнародних злочинів та інформаційна війна з Росією.Київ: Наш формат, 2022. 242 с.
11. Девід Е. Сенгер. Досконала зброя. Війна, саботаж і страх у кіберепоху. Пер. В. Дєдик. Львів: Астролябія, 2022. 496 с.

12. Дипломатія і цифрові технології: виклики та перспективи розвитку [Електронний ресурс] // *Український дипломатичний щорічник*. — 2023. — № 68. — Режим доступу: http://ud.gdip.com.ua/wp-content/uploads/2023/12/68_2023.pdf. — (Дата звернення: 18.10.2025).

13. Інформаційна безпека, IT-безпека, кібербезпека: у чому різниця? [Електронний ресурс] // *H-X Technologies*. — Режим доступу: https://www.h-x.technology/ua/blog-ua/infosec-itsec-cybersecurity-defference-ua. — (Дата звернення: 18.10.2025).

14. Кай-Фу Лі. Наддержави штучного інтелекту. Китай, Кремнієва долина і новий світовий лад. Пер. В. Пунько. Київ: BookChef, 2020. 297 с.

15. Кібердайджест. Липень 2024 [Електронний ресурс] // *Український фонд безпекових студій (UFSS)*. — Київ, 2024. — Режим доступу: https://ufss.com.ua/wp-content/uploads/2024/08/Cyber-digest_Jul_2024_UA.pdf. — (Дата звернення: 18.10.2025).

16. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології. Київ: Сідкон, 2022. 284 с.

17. Когут Ю. Цифрова трансформація економіки та проблеми кібербезпеки. Київ: Сідкон, 2021. 368 с.

18. Когут Ю. Штучний інтелект і безпека. Київ: Сідкон, 2024. 294 с.

19. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. 2010. № 3. С. 123–129.

20. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. Одеса: Юридична література, 2003. 471 с.

21. Луценко Ю. В., Тарасюк А. В., Денисенко М. М. Кібербезпека та інформаційна безпека: співвідношення понять [Електронний ресурс] // *Юридичний науковий електронний журнал*. — 2022. — № 8. — С. 295–299.

— Режим доступу: http://lsej.org.ua/8_2022/70.pdf. — (Дата звернення: 18.10.2025)

22. Макаренко Є.А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст // *Міжнародна інформаційна безпека: сучасні концепції і практика*. — 2023. — С. 51–59.

23. Міністерство закордонних справ України. *Стратегія публічної дипломатії України на 2021-2025 роки.* Київ: МЗС України, 2021. URL: https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%97/public-diplomacy-strategy.pdf - (дата звернення: 18.10.2025).

24. Кабінет Міністрів України. *Про затвердження Плану дій з реалізації Стратегії зовнішньополітичної діяльності України : Розпорядження Кабінету Міністрів України від 18 квітня 2023 р. № 327-р.* Київ: КМУ, 2023. URL: https://zakon.rada.gov.ua/laws/show/327-2023-%25D1%2580%23Text#Text - (дата звернення: 18.10.2025).

25. Омельяненко В. „Не лише навчатися, але й навчати: що забезпечує успіхи кібердипломатії України“. *Європейська правда*, 5 жовтня 2023. URL: https://www.eurointegration.com.ua/experts/2023/10/5/7170738/ - (дата звернення: 18.10.2025).

26. Міжнародна інформаційна безпека: сучасні виклики та загрози. К.: Центр вільної преси, 2006. 257 с.

27. Омельяненко В. Україна у цифровій дипломатії: нові горизонти міжнародного впливу [Електронний ресурс] // *Європейська правда*. — 2023. — Режим доступу: https://www.eurointegration.com.ua/experts/2023/10/5/7170738/. — (Дата звернення: 18.10.2025).

28. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення // *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. — 2021. — № 2 (37). — DOI: https://doi.org/10.37750/2616-6798.2021.2(37).238348.

29. Поляков О. М. Кібердипломатія як важливий напрямок міжнародно-правового співробітництва в умовах режиму воєнного стану [Електронний ресурс] // *National Law Journal*. — 2024. — № 6. — DOI: https://doi.org/10.51989/NUL.2024.6.10. — Режим доступу: https://orcid.org/0000-0002-8984-1476. — (Дата звернення: 18.10.2025).

30. Пугачов О.І. Зарубіжний досвід забезпечення інформаційної безпеки держави // *Актуальні проблеми міжнародних відносин та суспільних комунікацій*. — 2024. — № 13 (2). — С. 7–15. — DOI: https://doi.org/10.54929/2786-5746-2024-13-02-07.

31. Рассел С. Сумісний з людиною. Штучний інтелект і проблема контролю. Пер. В. Зенгва. Київ: BookChef, 2020. 416 с.

32. Скіннер К. Людина цифрова. Четверта революція в історії людства, яка торкнеться кожного. Харків: Фабула, 2020. 272 с.

33. Угода про співробітництво у сфері безпеки між Україною та Канадою // *Офіційне інтернет-представництво Президента України*. — 3 травня 2024 р. — [Електронний ресурс]. — Режим доступу: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89233 (дата звернення: 18.10.2025).

34. Україна долучилася до Глобальної угоди про співпрацю для безпечного розвитку ШІ // *MediaSapiens*. — 30 травня 2024 р. — [Електронний ресурс]. — Режим доступу: https://ms.detector.media/trendi/post/35078/2024-05-30-ukraina-doluchylasya-do-globalnoi-ugody-pro-spivpratsyu-dlya-bezpechnogo-rozvytku-shi/ (дата звернення: 18.10.2025).

35. Уряд України. Національна стратегія кібербезпеки України (Указ № 447/2021). Київ, 2021. URL: https://www.president.gov.ua/documents/4472021-40013

36. Федонюк С. В. *Міжнародні аспекти безпеки кіберпростору : монографія* / С. В. Федонюк. — Луцьк : Вежа-Друк, 2022. — 284 с.

37. Харарі Ю. Н. 21 урок для 21 століття. Київ: Book Chef, 2021. 416 с.

38. Харарі Ю. Н. Nexus. Коротка історія інформаційних мереж від кам'яного віку до ШІ. Пер. Н. Хаєцька. Київ: Book Chef, 2025. 640 с.

39. Шваб К. Четверта промислова революція. Формуючи четверту промислову революцію. Київ: Клуб сімейного дозвілля, 2019. 416 с.

40. Державна служба спеціального зв'язку та захисту інформації України (CERT-UA). Щорічний звіт з кібербезпеки 2023. Київ, 2023.

41. Anderson R., Moore T. The Economics of Information Security. Science. 2006. 314 (5799). P. 610–613.

42. Aven T. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research.* 2016. Vol. 253, No 1, pp. 1-13. DOI:10.1016/j.ejor.2015.12.023. URL: https://www.researchgate.net/publication/290010068_Risk_assessment_and_risk_management_Review_of_recent_advances_on_their_foundation/fulltext/56a022d808ae4af52546f5a1/Risk-assessment-and-risk-management-Review-of-recent-advances-on-their-foundation.pdf

43. Brundage M., Avin S., Clark J. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation. Oxford / University of Cambridge, 2018. URL: https://www.researchgate.net/publication/323302750_The_Malicious_Use_of_Artificial_Intelligence_Forecasting_Prevention_and_Mitigation

44. Cabinet Office Finland. (2024). Revised Cyber Security Strategy Responds to Changed Security Environment.URL: https://valtioneuvosto.fi/en/-/1410829/revised-cyber-security-strategy-responds-to-changed-security-environment (дата звернення: 16.10.2025).

45. Cabinet Office (UK). Cyber Security and Resilience Bill: Draft Framework and Consultation Summary. HM Government, London, 2024.

46. Cabinet Office (UK). *Government Cyber Security Strategy: 2022 to 2030.* London: Cabinet Office, January 2022. URL: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf
(дата звернення: 21.11.2025)

47. Cisco. The State of AI Security. URL: https://www.cisco.com/c/en/us/products/security/state-of-ai-security.html (дата звернення: 18.10.2025).

48. Council of Europe. *Convention 108+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised version).* Strasbourg: Council of Europe, 2018. 28 p. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
(дата звернення: 18.10.2025).

49. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 4 May 2016. 88 p. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
(дата звернення: 21.11.2025).

50. Council of Europe. *Convention on Cybercrime (ETS No 185 – Budapest Convention).* Strasbourg: Council of Europe, 23 Nov. 2001. — 25 с. URL: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

51. DataGuidance. (2025). Finland: Cybersecurity Act Enters into Force. URL: https://www.dataguidance.com/news/finland-cybersecurity-act-enters-force (дата звернення: 16.10.2025).

52. Enescu S. "A Comparative Study on European Cyber Security Strategies." *Redefining Community in Intercultural Context: RCIC'20.* Vol. 9, No 1 (2020), pp. 277-282. URL: https://www.afahc.ro/ro/rcic/2020/rcic'20/volum_2020/277-282%20Enescu.pdf

53. European Commission & High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade. JOIN(2020) 18 final, 16.12.2020.* Brussels: European Union, 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018

54. European Union Agency for Cybersecurity (ENISA). *2023 Consolidated Annual Activity Report.* Luxembourg: Publications Office of the European Union, June 2024. - 174 p. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/2023%20Consolidated%20Annual%20Activity%20Report_1.pdf

55. European Union Agency for Cybersecurity (ENISA). *National Cyber Security Strategies.* [Електронний ресурс]. URL: https://www.enisa.europa.eu/publications/cybe r-security-strategies-paper

56. European Parliament. *EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace. European Parliament Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure*

Cyberspace (2013/2606(RSP)), P7_TA(2013)0376. Official Journal of the European Union, C 93, 21 March 2014.

57. ENISA (European Union Agency for Cybersecurity). (2024). Finland: National Cybersecurity Action Plan 2024.URL: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/action-plans/FI_ACTION_PLAN_2024_en.pdf (дата звернення: 16.10.2025).
58. European Parliament and the Council of the European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*Official Journal of the European Union L 333, 27 Dec. 2022, pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (дата звернення: 16.10.2025).
59. Forrester Research, Inc.. *The Forrester Wave™: Zero Trust Platform Providers, Q3 2023.* Cambridge (MA): Forrester Research, Inc., 2023. URL: https://www.checkpoint.com/kr/downloads/resources/forrester-q3-2023-ztp.pdf (дата звернення: 18.10.2025).
60. European External Action Service (EEAS). *Cyber: EU and Japan hold 6th Cyber Dialogue in Tokyo.* Brussels: EEAS, 11 Nov. 2024. URL: https://www.eeas.europa.eu/eeas/cyber-eu-and-japan-hold-6th-cyber-dialogue-tokyo_en (дата звернення: 18.10.2025).
61. Gordon L. A., Loeb M. P. The Economics of Information Security Investment. ACM TISSEC. 2002. 5 (4). P. 438–457.
62. Pérez Alvarez M., Havens J., Winfield A. *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Artificial Intelligence and Autonomous Systems.* Version 1.0. New York: IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 2017.

63. International AI Safety Report 2025. UK Government. URL: https://www.gov.uk/government/publications/international-ai-safety-report-2025/international-ai-safety-report-2025#risks-from-malicious-use (дата звернення: 18.10.2025).
64. International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024. Geneva: ITU. URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (дата звернення: 16.10.2025).
65. Into Digital. (2025). Cybersecurity: The NIS2 Directive Takes Effect in Finland. URL: https://into-digital.fi/en/cybersecurity-the-nis2-directive-takes-effect-in-finland/ (дата звернення: 16.10.2025).
66. ISO/IEC. ISO/IEC 27001: Information Security Management Systems — Requirements. Geneva, 2022. URL: https://www.iso.org/standard/27001 (дата звернення: 16.10.2025).
67. ISO/IEC. *Information technology — Security techniques — Information security risk management. ISO/IEC 27005:2018 (E).* Geneva: ISO/IEC, 2018. — 56 с. URL: https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027005-2018.pdf (дата звернення: 16.10.2025).
68. ISO/IEC. *ISO/IEC 27032:2023 — Cybersecurity — Guidelines for Internet security.* Geneva: ISO/IEC, 2023. — 28 с. URL: https://www.iso.org/standard/76070.html (дата звернення: 16.10.2025).
69. International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) v5.* Geneva: ITU D-Cybersecurity Programme, 2024. — 260 с. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (дата звернення: 21.11.2025).
70. Kleijssen J., Perri P. Cybercrime, Evidence and Territoriality: Issues and Options. Journal of Cyber Policy. 2017. 2 (2). P. 208–226.

71. Ministry for Foreign Affairs of Finland. (2025). Cyber Security and the Cyber Domain. URL: https://um.fi/cyber-security-and-the-cyber-domain (дата звернення: 16.10.2025).
72. Mueller, M. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010. 320 p. URL: http://ndl.ethernet.edu.et/bitstream/123456789/53494/1/1.Milton%20L.%20Mueller.pdf (дата звернення: 21.11.2025)
73. National Cyber Security Centre. *Annual Review 2024.* London: NCSC, 2024 URL: https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf (дата звернення: 21.11.2025)
74. National Cyber Security Centre. *Annual Review 2025.* London: NCSC, 2025. URL: https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf (дата звернення: 21.11.2025)
75. National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD: NIST, January 2023. URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (doi 10.6028/NIST.AI.100-1) (дата звернення: 21.11.2025).
76. National Institute of Standards and Technology. Guide for Conducting Risk Assessments (SP 800-30). Gaithersburg, 2012. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (дата звернення: 21.11.2025).
77. NATO. Cyber Defence Pledge. Brussels, 2016. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge (дата звернення: 21.11.2025).
78. NATO Cooperative Cyber Defence Centre of Excellence. *The NATO CCDCOE welcomes new members Iceland, Ireland, Japan and Ukraine.* Tallinn: CCDCOE, 2023. URL: https://ccdcoe.org/news/2023/the-nato-ccdcoe-

welcomes-new-members-iceland-ireland-japan-and-ukraine/ (дата звернення: 21.11.2025).

79. NATO Allied Command Transformation. *Cyber Defence* [Електронний ресурс]. URL: https://www.act.nato.int/activities/cyber/ (дата звернення: 21.11.2025).
80. Nye J. S. Cyber Power. Harvard Kennedy School, Belfer Center, 2010. URL: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf (дата звернення: 21.11.2025).
81. Nye J. S. Deterrence and Dissuasion in Cyberspace. International Security. 2017. 41 (3).
82. OECD. *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity.* Paris: OECD Publishing, 2022. URL: https://doi.org/10.1787/a69df866-en (дата звернення: 21.11.2025).
83. OECD. *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.* Paris: OECD Publishing, 2015. URL: https://doi.org/10.1787/9789264245471-en (дата звернення: 21.11.2025).
84. Polyakova A., Fried D. Democratic Defense Against Disinformation. Atlantic Council, 2022. URL: https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf (дата звернення: 18.10.2025).
85. Radanliev P. Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains and Quantum Computing. Journal of Cyber Security Technology. 2025. 9 (1). P. 28–78. DOI: 10.1080/23742917.2024.2312671 (дата звернення: 18.10.2025).
86. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020.

87. Schmitt MN. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press, 2017. URL: https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf (дата звернення: 18.10.2025).
88. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World. New York: Norton, 2018. URL: https://www.scribd.com/document/753921128/Click-Here-to-Kill-Everybody-Security-and-Survival-in-a-Hyper-Connected-World (дата звернення: 21.11.2025).
89. SCO Secretariat. Shanghai Cooperation Organisation Declaration on International Information Security.Samarkand, 16 September 2022. URL: https://eng.sectsco.org/files/914622/914622 (дата звернення: 21.11.2025).
90. Singer P. W., Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford; New York: Oxford University Press, 2014. URL: https://api.pageplace.de/preview/DT0400.9780199918102_A23618218/preview-9780199918102_A23618218.pdf (дата звернення: 21.11.2025).
91. Thomas T. Information Warfare in the Second (1997) US-Russian Summit. Military Review. 2001. 81 (4). P. 47–55.
92. Tikk-Ringas E. Developments in the Field of Information and Telecommunications in the Context of International Security: Work of the UN First Committee 1998-2012. Geneva: ICT4Peace, 2012. URL: https://citizenlab.org/wp-content/uploads/2012/08/UN-GGE-Brief-2012.pdf. (дата звернення: 21.11.2025).
93. Tortoise Media. The Global AI Index. URL: https://www.tortoisemedia.com/intelligence/global-ai/ (дата звернення: 18.10.2025).

94. UK Government. *The UK's International Technology Strategy. CP 810.* London: His Majesty's Government, March 2023. URL: https://data.parliament.uk/DepositedPapers/Files/DEP2023-0272/The_UKs_International_Technology_Strategy.pdf (дата звернення: 21.11.2025).

95. Cabinet Office (UK). *The UK Integrated Review Refresh 2023: Responding to a More Contested and Volatile World* (Ref. CP 811). London: His Majesty's Government, 13 March 2023. URL: https://assets.publishing.service.gov.uk/media/641d72f45155a2000c6ad5d5/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf (дата звернення: 21.11.2025)

96. United Nations. General Assembly Resolution A/RES/73/266 "Advancing responsible State behaviour in cyberspace in the context of international security". New York: United Nations, 2 Jan. 2019. URL: https://www.un.org/en/ga/73/resolutions.shtml (дата звернення: 21.11.2025)

97. United Nations. *Developments in the field of information and telecommunications in the context of international security. Report of the First Committee, A/75/394-EN.* New York: United Nations, 16 Nov. 2020. URL: https://digitallibrary.un.org/record/3892631?ln=en&v=pdf (дата звернення: 21.11.2025)

98. United Nations. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)*. New York: United Nations, 22 July 2015. URL: https://digitallibrary.un.org/record/799853?ln=en&v=pdf (дата звернення: 21.11.2025).

99. United Nations General Assembly. Resolution 53/70 "Developments in the Field of Information and Telecommunications in the Context of International

Security” and Its Influence on the International Rule of Law in Cyberspace. SSRN Electronic Journal. 2021. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3856900 (дата звернення: 18.10.2025).

100. U.S. Department of State. Proceedings of the 2023 U.S.–Ukraine Cyber Dialogue. Washington, D.C., 2023. URL: https://2021-2025.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue (дата звернення: 21.11.2025)

101. Zadeh L. A. Fuzzy Sets // *Fuzzy Sets, Fuzzy Logic, Fuzzy Systems*. — Singapore : World Scientific Publishing Co. Inc., 1996. — С. 394–432.

АНОТАЦІЯ

Кочанов В.В Глобальні виклики інформаційної безпеки (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 75 с. (рукопис).

Магістерська кваліфікаційна робота аналізує глобальні виклики у сфері міжнародної інформаційної безпеки в XXI столітті, зумовлені швидким розвитком цифрових технологій і штучного інтелекту. У ній розглядається еволюція поняття цієї безпеки та зміни у безпекових парадигмах під впливом цифровізації, автоматизації, Інтернету речей і генеративних моделей ШІ.

На основі порівняльного аналізу розглянуто підходи України, Великої Британії та Фінляндії до формування національних стратегій кібербезпеки та кібердипломатії. Показано, що ці країни по-різному структурують організаційні моделі реагування, однак мають спільні риси — орієнтацію на багаторівневу співпрацю, зміцнення стійкості, розбудову професійних спроможностей, інтеграцію міжнародних стандартів та активну участь у багатосторонніх форматах. Підкреслено, що ефективність протидії цифровим загрозам залежить не лише від національних механізмів, а й від міжнародної координації, обміну даними та формування універсальних норм відповідальної поведінки держав у кіберпросторі.

Результати роботи підтверджують необхідність міждисциплінарного підходу до дослідження інформаційних ризиків та демонструють важливість стратегічного партнерства. Отримані висновки можуть бути використані для модернізації державної інформаційної політики, підвищення цифрової стійкості суспільства та вдосконалення міжнародного співробітництва у сфері кібербезпеки.

Ключові слова: глобальне врядування, дезінформація, діпфейк, інформаційна безпека, інформаційні ризики, кібердипломатія, кіберзагрози, критична інфраструктура, штучний інтелект, цифрові технології, кібердипломатія, міжнародна безпека.

ANNOTATION

Kochanov V.V. Global challenges to information security in the 21st century (master’s work). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 75 p. (manuscript).

The master's dissertation examines global challenges in the field of international information security in the 21st century caused by the rapid development of digital technologies and artificial intelligence. This research explores the evolution of the concept of information security and changes in security paradigms under the influence of digitalisation, automation, the Internet of Things, and generative AI models.

Through a comparative analysis, the approaches of Ukraine, the United Kingdom, and Finland to the formation of national cybersecurity and cyber diplomacy strategies are analysed. It is shown that these countries structure their organisational response models differently, yet they share common features: a focus on multi-level cooperation, strengthening resilience, building professional capacity, integrating international standards, and actively participating in multilateral formats. Moreover, the effectiveness of countering digital threats depends not only on national mechanisms but also on international coordination, data exchange, and the formation of universal norms of responsible behaviour by states in cyberspace.

The results of the research confirm the need for an interdisciplinary approach to the study of information risks and demonstrate the importance of strategic partnerships. The findings can be used to modernise state information policy, increase the digital resilience of society and improve international cooperation in the field of cybersecurity.

Keywords: artificial intelligence, cyber diplomacy, cyber threats, critical infrastructure, deepfakes, digital technologies, disinformation, global governance, information risks, information security, information risks, international security.

ВІДГУК
керівника кваліфікаційної роботи магістра
студента 2–го курсу, групи УМІБ–61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Навчально-науковий інститут
«Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Кочанова Володимира Валерійовича
на тему **«Глобальні виклики інформаційної безпеки у XXI столітті»**

1. Актуальність дослідження зумовлена тим, що стрімкий розвиток цифрових технологій та використання штучного інтелекту створюють нові загрози для глобальної інформаційної безпеки, які виходять далеко за межі технічної сфери та набувають стратегічного виміру. Приклади застосування технологій deepfake у гібридній війні проти України наочно демонструють, як інформаційні атаки стають інструментом політичного впливу та дестабілізації суспільств. У цьому контексті дослідження має особливу значущість для України, адже воно дозволяє осмислити сучасні виклики та виробити ефективні механізми міжнародної співпраці й національної стійкості в умовах війни та цифрової трансформації.

2. Сильними сторонами роботи є самостійна авторська позиція у визначенні сучасних викликів та міжнародних механізмів протидії кіберзагрозам, міждисциплінарний підхід до аналізу інформаційної безпеки, що поєднує право, етику, міжнародні відносини та технології, а також акцент на парадигмальних змінах у розумінні безпеки як системного процесу підтримання стабільності соціально-технічних систем. Автор вдало інтегрує приклади впливу новітніх технологій (ШІ, IoT, Big Data, хмарні обчислення), демонструє практичну значущість українського досвіду в умовах гібридної війни та водночас розглядає міжнародний контекст, включаючи ініціативи ООН, ЄС і НАТО. Важливою перевагою є прогностичний вимір дослідження, що окреслює напрями майбутньої політики та науки, а також практична корисність висновків для державних діячів і науковців у розробці адаптивних стратегій кібербезпеки.

3. Запропоновані здобувачем заходи та пропозиції вирізняються системністю й практичною спрямованістю. Вони ґрунтуються на комплексному аналізі сучасних технологічних тенденцій та міжнародних механізмів кіберзахисту, що забезпечує їхню актуальність і прикладну цінність для організації. Особливо важливим є акцент на міждисциплінарному підході та інтеграції національного й міжнародного досвіду, що створює реальні перспективи використання напрацьованих рекомендацій у стратегічному плануванні, розвитку партнерств та підвищенні інституційної стійкості.

4. Недоліки роботи. Попри логічну структурованість та ґрунтовність роботи, усе ж у ній простежуються певні недоліки. Автор надмірно зосереджується на нормативно-правових та інституційних аспектах міжнародної інформаційної безпеки, що створює враження формалізованості й обмежує аналітичну новизну дослідження. Водночас бракує розгорнутого аналізу соціально-психологічного виміру інформаційних загроз, зокрема їхнього впливу на суспільну довіру, поведінку громадян та демократичні процеси. Обмежений глобальний контекст, зосереджений переважно на ЄС, НАТО та ООН, також зменшує універсальність висновків. Крім того, рекомендації мають концептуальний характер і не завжди супроводжуються конкретними механізмами практичної реалізації. Ці аспекти окреслюють напрями для подальшого вдосконалення та розширення прикладної значущості роботи.

5. Загальний висновок і оцінка кваліфікаційної роботи, присвоєння кваліфікації. Загалом представлена кваліфікаційна робота є цілісним і завершеним дослідженням, що вирізняється актуальністю тематики та ґрунтовним аналізом сучасних викликів міжнародної інформаційної безпеки у цифрову епоху. Автор переконливо демонструє еволюцію поняття інформаційної безпеки, розкриває вплив новітніх технологій та штучного інтелекту на формування глобальних ризиків, а також аналізує роль міжнародних інституцій і кібердипломатії у протидії загрозам. Сильними сторонами роботи є міждисциплінарний підхід, поєднання теоретичних і практичних аспектів, використання українського досвіду в умовах гібридної війни та інтеграція міжнародного контексту. Водночас дослідження має певні

недоліки, зокрема надмірну концентрацію на нормативно-інституційному аналізі та недостатнє висвітлення соціально-психологічного виміру інформаційних загроз. Попри це, робота відповідає вимогам, що висуваються до кваліфікаційних досліджень, і може бути оцінена як вагомий науковий та практичний внесок у розуміння сучасних проблем глобальної інформаційної безпеки, а її автор Кочанов Володимир Валерійович, заслуговує на оцінку 90 балів «відмінно» та присвоєння кваліфікації магістра за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

Керівник кваліфікаційної роботи,
доктор політичних наук, доцент
завідувач кафедри міжнародних відносин
Навчально-наукового інституту
«Каразінський інститут міжнародних відносин та
туристичного бізнесу»
Харківського національного
університету імені В.Н. Каразіна Наталія ВІННИКОВА

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2–го курсу, групи УМІБ–61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Навчально-науковий інститут
«Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Кочанова Володимира Валерійовича
на тему «Глобальні виклики інформаційної безпеки у XXI столітті»

1. **Актуальність** цієї кваліфікаційної роботи обумовлена швидким розвитком цифрових технологій, які одночасно відкривають нові можливості та створюють великі ризики для інформаційної безпеки держав, суспільств і міждержавних систем. У XXI столітті штучний інтелект, великі дані, Інтернет речей, хмарні сервіси та інші технології значно змінюють характер глобальних загроз, прискорюючи появу нових форм кібератак, дезінформації, втручань у виборчі процеси і маніпуляцій у цифровому середовищі. В умовах сучасності дослідження інформаційної безпеки, моделей міжнародної реакції, національних стратегій і кібердипломатії стає особливо актуальним, адже жодна країна сама не здатна боротися з комплексними цифровими викликами. З цієї причини робота є своєчасною, практично спрямованою та важливою для сучасної науки міжнародних відносин і безпеки.

2. **Характеристика якості виконання кожного розділу роботи**

У **першому розділі** роботи автором ретельно розкрито теоретико-методологічні засади міжнародної інформаційної безпеки, визначено етапи її еволюції та проаналізовано вплив цифровізації на трансформацію класичних безпекових парадигм. Подано огляд ключових наукових підходів до вивчення інформаційних ризиків, що забезпечило концептуальну цілісність та методологічну глибину розділу.

Другий розділ кваліфікаційної роботи присвячено дослідженню глобальних

технологічних тенденцій і ризиків, пов'язаних із використанням цифрових технологій та штучного інтелекту. На особливу увагу заслуговує глибокий аналіз ризиків ШІ. Важливо, що автор підкріпив аналіз посиланнями на актуальні міжнародні звіти, включно з International AI Safety Report 2025.

У **третьому розділі** автором докладно розглянуто національні та міжнародні моделі реагування на інформаційні загрози, представлено порівняльний аналіз стратегій України, Великої Британії та Фінляндії. Вдалим є акцент на ролі кібердипломатії, взаємодії держав у рамках ООН, НАТО, ЄС та спеціалізованих програм, а також визначення перспектив формування глобального нормативного середовища для безпечного розвитку цифрових технологій.

3. **Ступінь обґрунтованості висновків роботи**

Висновки є логічними, аргументованими та повністю відповідають меті й завданням дослідження. Автор обґрунтовано доводить, що інформаційна безпека в умовах цифрової епохи вимагає міждисциплінарного підходу, міжнародної координації та адаптивних політик. Важливо, що висновки містять практичні рекомендації для державної політики України та подальшої кібердипломатичної діяльності.

4. **Характеристика ілюстративної частини роботи**

Ілюстративна частина у роботі відсутня. Хоча її включення могло б посилити аналітичний аспект, відсутність графічного матеріалу не впливає на загальну наукову цінність тексту.

5. У роботі використано широке коло актуальних вітчизняних та міжнародних джерел, включно зі стратегічними документами України, Великої Британії, Фінляндії, звітами ENISA, ITU, NATO, OEWG та іншими. Автором залучено сучасні дослідницькі методи: порівняльний аналіз, системний підхід, елемент аналізу ризиків та стратегічного прогнозування, що відповідає високим академічним стандартам.

6. **Позитивні сторони роботи**. До позитивних аспектів належать системність дослідження, глибокий аналіз технологічних ризиків, логічність викладу, послідовна аргументація та використання актуальної доказової бази. Особливо слід відзначити ґрунтовний порівняльний аналіз трьох держав, а також якісне розкриття тематики кібердипломатії, що часто залишається поза увагою інших дослідників.

7. **Недоліки роботи**. Основним недоліком можна вважати відсутність графічних матеріалів, які могли б підсилити окремі аналітичні положення. Водночас цей аспект не зменшує наукової цінності отриманих результатів.

8. **Практичне значення роботи** полягає у тому, що її висновки та надані автором рекомендації роботи можуть бути використані державними структурами, аналітичними центрами та органами зовнішньої політики у формуванні стратегій інформаційної безпеки та цифрової стійкості. Матеріали роботи є корисними у навчальному процесі з дисциплін міжнародної безпеки, кіберполітики та міжнародних відносин.

9. **Загальна оцінка кваліфікаційної роботи**. Кваліфікаційна робота Кочанова Володимири Валерійовича «Глобальні виклики інформаційної безпеки у XXI столітті» є самостійним, ґрунтовним і сучасним дослідженням, яке комплексно висвітлює поняття міжнародної інформаційної безпеки, проблеми кіберзагроз, цифрової трансформації та міжнародної співпраці. Робота вирізняється високим рівнем теоретичної підготовки, якістю аналітичної частини та актуальністю практичних висновків і заслуговує на позитивну оцінку 85 балів.

Рецензент:
доцент закладу вищої освіти
кафедри політичної соціології
Харківського національного
університету імені В. Н. Каразіна,
кандидат соціологічних наук В'ячеслав НІКУЛІН