КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

Кафедра міжнародного та приватного права

КВАЛІФІКАЦІЙНА РОБОТА

за темою:

«ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРОПЕРАЦІЇ В МІЖНАРОДНОМУ ГУМАНІТАРНОМУ ПРАВІ»

Виконав:
здобувач 2 курсу, групи ММ-21з
спеціальності 293 «Міжнародне право»
Іванюк Микола Миколайович
(П.І.Б. здобувача)

Науковий керівник:
Пилипенко Володимир Пилипович
доцент кафедри міжнародного та приватного права
КУП НАН України
(П.І.Б., науковий ступінь, вчене звання, посада)

Робота допущена до захисту в ЕК
«__» _____2026 р.

В.о. завідувача кафедри Чернега В. М.,
доктор юридичних наук, професор
(П.І.Б., науковий ступінь, вчене звання, посада)

КИЇВ-2026

Реєстрація

номер дата підпис в.о. завідувача кафедри

Рекомендовано до захисту

підпис наукового керівника ініціали, прізвище наукового керівника

Результат захисту

оцінка дата захисту

Голова ЕК

підпис ініціали, прізвище

Члени ЕК

підпис ініціали, прізвище

підпис ініціали, прізвище

підпис ініціали, прізвище

підпис ініціали, прізвище

Секретар ЕК

підпис ініціали, прізвище

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ
НАУК УКРАЇНИ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ІЗ ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється студент Іванюк Микола Миколайович до захисту кваліфікаційної роботи

Освітній ступінь «Магістр»

Спеціальність 293 «Міжнародне право» Галузь знань: 29 «Міжнародні відносини»

На тему: «Відповідальність за кібероперації в міжнародному гуманітарному праві».

Кваліфікаційна робота і рецензія додаються.

В.о. завідувача кафедри міжнародного та приватного права КУП НАН України, д.ю.н., професор _____В. М. Чернега

Довідка про успішність

Іванюк Микола Миколайович за період навчання зі спеціальності 293 «Міжнародне право» з 2024 року до 2026 року повністю виконав навчальний план із таким розподілом оцінок за:

національною шкалою: відмінно ____%, добре ____%, задовільно _____%; шкалою ЄКТС: A _____%; B _____%; C _____%; D _____%; E _____%.

Методист _____

Висновок керівника кваліфікаційної роботи

Студент Іванюк Микола Миколайович вчасно виконав поставлені перед ним науковим керівником завдання щодо виконання кваліфікаційної роботи на тему «Відповідальність за кібероперації в міжнародному гуманітарному праві», у повному обсязі розкрив зміст заявленої теми дослідження, чітко дотримувався вимог структуризації і оформлення роботи відповідно до методичних рекомендацій з виконання і захисту кваліфікаційних робіт здобувачів другого (магістерського) рівня вищої освіти зі спеціальності 293 «Міжнародне право» Київського університету права Національної академії наук України. З огляду на відсутність значних недоліків дослідження кваліфікаційну роботу М.М.Іванюк може бути допущено до захисту.

Науковий керівник _____ В.П.Пилипенко.

«____» _____2026 року

Висновок кафедри міжнародного та приватного права КУП НАНУ на кваліфікаційну роботу

Кваліфікаційну роботу розглянуто. Студент Іванюк М.М. допускається до захисту цієї роботи в Екзаменаційній комісії.

В.о. завідувача кафедри міжнародного та приватного права_____ В. М Чернега_____ »_____2026 року

КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА НАН УКРАЇНИ

Кафедра міжнародного та приватного права
Освітній ступінь: «Магістр»
Спеціальність 293 «Міжнародне право»
Галузь знань 29 «Міжнародні відносини»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри

_____
_____

(підпис)
«_____» _____20____року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
Іванюка Миколи Миколайовича

1.Тема роботи: «Відповідальність за кібероперації в міжнародному гуманітарному праві»
Науковий керівник роботи Пилипенко В.П., доцент кафедри міжнародного та приватного права КУП НАН України

2. Строк подання студентом роботи «_____» _____20_____року

3. Вихідні дані до роботи Нормативно-правову основу дослідження становлять міжнародні договори, Статут Організації Об'єднаних Націй, Женевські конвенції 1949 року та додаткові протоколи до них, міжнародні акти у сфері кібербезпеки, документи ООН, НАТО та Європейського Союзу, Талліннський посібник 2.0, національне законодавство України у сфері кібербезпеки, міжнародного гуманітарного права та міжнародно-правової відповідальності.
Теоретичну основу роботи складають наукові праці вітчизняних та зарубіжних учених у сфері міжнародного гуманітарного права, міжнародної безпеки, кіберправа та міжнародно-правової відповідальності держав.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

1. Поняття та сутність кібероперацій.
2. Джерела міжнародного гуманітарного права у сфері кібероперацій.
3. Кваліфікація кібероперацій як збройного нападу.
4. Підстави відповідальності держав.
5. Форми та види міжнародно-правової відповідальності.
6. Індивідуальна кримінальна відповідальність.
7. Сучасні міжнародні ініціативи та практика регулювання кібероперацій в умовах збройних конфліктів.
8. Проблеми та напрями вдосконалення норм міжнародного гуманітарного права щодо кібероперацій.
9. Практика кібероперацій у російсько-українській війні та проблеми притягнення до міжнародно-правової відповідальності.

Розділи	Прізвище та ініціали, посада керівника	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Пилипенко В.П., доцент, доцент кафедри міжнародного та приватного права КУП НАН України		
Розділ 2	Пилипенко В.П. доцент, доцент кафедри міжнародного та приватного права КУП НАН України		
Розділ 3	Пилипенко В.П., доцент, доцент кафедри міжнародного та приватного права КУП НАН України		

5. Дата видачі завдання: _____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Погодження плану та підбір джерел	до 20.03.2026	виконано
2.	Написання вступу та І розділу кваліфікаційної роботи	до 02.04.2026	виконано
3.	Написання ІІ розділу кваліфікаційної роботи	до 24.04.2026	виконано
4.	Написання ІІІ розділу кваліфікаційної роботи та подання завершеної роботи студентом науковому керівнику	до 18.05.2026	виконано
5.	Реєстрація кваліфікаційної роботи на кафедрі	до 23.05.2026	виконано
6.	Попередній захист кваліфікаційної роботи на кафедрі	до 25.05.2026	виконано
7.	Оформлення письмового відгуку наукового керівника, зовнішньої рецензії та допуск кафедрою кваліфікаційної роботи до захисту в ЕК	до 05.06.2026	виконано

Здобувач(ка) вищої освіти _____Іванюк М.М.
(підпис)

Керівник роботи _____ **Пилипенко В.П.**
(підпис)

ВІДГУК
наукового керівника доцента Пилипенка В.П.
на кваліфікаційну роботу Іванюка Миколи Миколайовича
на тему: «Відповідальність за кібероперації в міжнародному гуманітарному праві»

Актуальність теми, стан розробки наукової проблеми, визначення мети й напрямків виконання роботи.

Щодо актуальності теми роботи магістранта Іванюка Миколи Миколайовича, то вона без сумніву є актуальною, оскільки пов'язана з необхідністю комплексного дослідження проблем міжнародно-правової відповідальності за кібероперації в умовах стрімкого розвитку цифрових технологій, трансформації сучасних збройних конфліктів та активного використання кіберпростору як нового середовища міжнародного протистояння. Особливої актуальності зазначена проблематика набуває в умовах російсько-української війни, під час якої кібероперації стали одним із ключових інструментів впливу на критичну інфраструктуру, інформаційні системи та безпекове середовище держави. У зв'язку з цим особливої уваги потребують питання застосування норм міжнародного гуманітарного права до кібероперацій, визначення підстав міжнародно-правової відповідальності держав та вдосконалення механізмів правового регулювання у цій сфері.

Щодо стану розробки наукової проблеми, то у Вступі надано реферативний огляд теоретичних джерел, необхідних для проведення дослідження, проаналізовано праці українських та зарубіжних науковців, міжнародно-правові акти, документи Організації Об'єднаних Націй, Талліннський посібник 2.0, а також національне законодавство України у сфері кібербезпеки та міжнародного гуманітарного права. Разом з тим магістрантом акцентовано увагу на тому, що сучасний стан міжнародно-правового регулювання кібероперацій характеризується фрагментарністю та відсутністю єдиного універсального підходу до визначення правової природи кібероперацій і механізмів відповідальності за них. Саме тому особливої уваги потребує проведення комплексного аналізу проблем міжнародно-правової відповідальності за кібероперації в умовах сучасних безпекових викликів та розвитку міжнародного гуманітарного права.

Щодо визначення мети й напрямків виконання роботи, то магістрантом взято для дослідження проблемні питання міжнародно-правової відповідальності за кібероперації, особливості застосування норм міжнародного гуманітарного права до кіберпростору, а також проблеми кваліфікації кібероперацій як форми застосування сили або збройного нападу з метою формування відповідних пропозицій щодо вдосконалення міжнародно-правового регулювання у цій сфері.

З цією метою:

У першому розділі проведено науковий аналіз поняття та сутності кібероперацій у міжнародному праві, досліджено правову природу кібероперацій у системі міжнародного гуманітарного права, а також проаналізовано питання кваліфікації кібероперацій як застосування сили або збройного нападу. На підставі проведеного дослідження зроблено ряд слушних теоретичних висновків щодо особливостей правового статусу кібероперацій у сучасному міжнародному праві.

У другому розділі магістрантом визначено підстави міжнародно-правової відповідальності держав за кібероперації, досліджено форми та види міжнародно-правової відповідальності, а також проаналізовано питання індивідуальної кримінальної відповідальності за кібероперації. За результатами проведеного дослідження зроблено ряд слушних висновків та пропозицій щодо вдосконалення механізмів міжнародно-правового реагування на кіберзагрози.

У третьому розділі проведено аналіз сучасних міжнародних ініціатив та практики регулювання кібероперацій, визначено проблеми вдосконалення міжнародного гуманітарного права у сфері кібероперацій, а також досліджено практику кібероперацій у російсько-українській війні та питання міжнародно-правової відповідальності за їх здійснення. Особливу увагу приділено перспективам розвитку міжнародного співробітництва у сфері кібербезпеки та необхідності адаптації міжнародного права до сучасних цифрових викликів.

При написанні роботи студентом використовувалися наукові методи, які дали йому можливість проаналізувати та систематизувати відповідний матеріал, провести комплексний аналіз міжнародного та національного законодавства, дослідити особливості правового регулювання кібероперацій та сформулювати висновки, які мають істотне значення для науки міжнародного права та міжнародного гуманітарного права.

Щодо висновків роботи, то особливу увагу звернено на проблеми застосування норм міжнародного гуманітарного права до кібероперацій, необхідність удосконалення механізмів міжнародно-правової відповідальності, а також потребу формування єдиних міжнародних підходів до правового регулювання діяльності держав у кіберпросторі.

Щодо впровадження результатів кваліфікаційної роботи, то окремі положення випускної кваліфікаційної роботи були апробовані у наукових виступах та можуть бути використані у навчальному процесі, науково-дослідній діяльності, правотворчій діяльності та практиці міжнародного співробітництва у сфері кібербезпеки.

Усі завдання згідно календарного плану, які поставив перед собою студент, виконані. При написанні кваліфікаційної роботи використано значну кількість міжнародно-правових актів, нормативно-правових джерел, наукової та навчальної літератури.

Всі зауваження наукового керівника були враховані.

Крім того, при написанні роботи магістрант був ознайомлений науковим керівником з Положенням про систему виявлення та запобігання академічному плагіату, йому була роз'яснена його сутність та наслідки, що він підтвердив.

Кваліфікаційна робота відповідає вимогам академічної доброчесності.

Кваліфікаційна робота Іванюка Миколи Миколайовича на тему: «Відповідальність за кібероперації в міжнародному гуманітарному праві» відповідає усім вимогам, які пред'являються до такого роду робіт, а тому може бути рекомендована кафедрою до публічного захисту в Екзаменаційній комісії.

Науковий керівник, доцент кафедри
міжнародного права та
галузевих правових дисциплін
права КУП НАН України Пилипенко В.П.

Отже за змістовну частину кваліфікаційної роботи можна поставити 70 балів.

РЕЦЕНЦІЯ

на кваліфікаційну (магістерську) роботу здобувача другого (магістерського) рівня вищої освіти спеціальності 293 «Міжнародне право» Іванюка Миколи Миколайовича на тему: **«Відповідальність за кібероперації в міжнародному гуманітарному праві»**

Кваліфікаційна робота Іванюка Миколи Миколайовича присвячена актуальній та важливій проблематиці міжнародного гуманітарного права, а саме дослідженню міжнародно-правової відповідальності за кібероперації в умовах сучасних міжнародних збройних конфліктів.

Актуальність теми магістерської роботи зумовлена стрімким розвитком цифрових технологій та трансформацією кіберпростору у самостійну сферу реалізації державної політики, включаючи сферу міжнародної безпеки та оборони. У сучасних умовах кібероперації дедалі частіше використовуються як інструмент впливу у міжнародних відносинах та здатні спричиняти наслідки, співмірні з наслідками традиційних форм застосування сили. Особливої актуальності дана проблематика набуває в умовах сучасних збройних конфліктів, зокрема російсько-української війни, де кібероперації стали невід'ємним елементом комплексного впливу на державу, її критичну інфраструктуру та інформаційні системи.

З цією метою студентом у Розділі 1 «Теоретико-правові засади кібероперацій у міжнародному гуманітарному праві» розкрито поняття та сутність кібероперацій, проаналізовано правову природу кібероперацій у системі міжнародного гуманітарного права, а також досліджено проблеми застосування норм міжнародного гуманітарного права до кібероперацій. Значну увагу приділено питанням кваліфікації кібероперацій як форми застосування сили або збройного нападу, а також особливостям реалізації принципів міжнародного гуманітарного права у кіберпросторі.

У Розділі 2 «Міжнародно-правова відповідальність за кібероперації» досліджено підстави міжнародно-правової відповідальності держав за здійснення кібероперацій, проаналізовано форми та види міжнародно-правової відповідальності, а також розглянуто питання індивідуальної кримінальної відповідальності за міжнародно-протиправні діяння у кіберпросторі. Автором обґрунтовано складність притягнення до відповідальності у зв'язку з проблемою атрибуції кібератак та участю недержавних суб'єктів у здійсненні кібероперацій.

У Розділі 3 «Розвиток міжнародно-правових механізмів відповідальності за кібероперації: проблеми та практика сучасних збройних конфліктів» студентом проаналізовано сучасні міжнародні ініціативи та практику регулювання кібероперацій в умовах збройних конфліктів, визначено проблеми та напрями вдосконалення норм міжнародного гуманітарного права щодо кібероперацій, а також досліджено практику кібероперацій у російсько-

українській війні та проблеми притягнення до міжнародно-правової відповідальності.

Студентом проаналізовано значну кількість міжнародно-правових актів, наукової літератури, аналітичних досліджень та практики міжнародних організацій. Правильно сформульовано об'єкт, предмет та мету дослідження, використано комплекс наукових методів, що дало можливість виконати поставлені завдання та сформулювати обґрунтовані висновки, які можуть бути використані у науковій діяльності, правотворчій практиці та навчальному процесі.

Проте, робота не позбавлена певних недоліків:

1. Аналізуючи правову природу кібероперацій та їх місце у системі міжнародного гуманітарного права, студентом недостатньо чітко висловлено власну позицію щодо критеріїв відмежування кібероперацій від інших форм інформаційного та цифрового впливу у міжнародних відносинах.
2. У Розділі 2 при дослідженні міжнародно-правової відповідальності держав значна увага приділена теоретичним аспектам правового регулювання, тоді як практику міжнародного реагування на конкретні кібератаки та діяльність міжнародних судових органів висвітлено менш детально, що певною мірою створює дисбаланс між теоретичною та практичною складовою дослідження.
3. У роботі використано значну кількість нормативних джерел та наукової літератури, проте окремі сучасні міжнародні аналітичні дослідження та практичні кейси щодо кібероперацій останніх років могли б бути проаналізовані більш ґрунтовно.
4. Хотілося б під час захисту заслухати позицію студента щодо перспектив формування універсального міжнародного договору у сфері регулювання кібероперацій, а також щодо практичної можливості створення ефективного міжнародного механізму атрибуції кібератак та притягнення винних суб'єктів до відповідальності.

Позитивним у роботі є комплексний аналіз міжнародно-правових аспектів кібероперацій, дослідження особливостей застосування норм міжнародного гуманітарного права у кіберпросторі, а також аналіз сучасних міжнародних викликів у сфері кібербезпеки та міжнародної відповідальності.

Робота нараховує значну кількість використаних джерел.

Це дає підстави рецензенту зробити висновок, що робота на тему: «Відповідальність за кібероперації в міжнародному гуманітарному праві» має завершений характер, відповідає вимогам, які пред'являються до такого роду робіт, та може бути оцінена на «відмінно» з урахуванням публічного захисту в ЕК.

Рецензент
к.ю.н., доцент

Анотація

Іванюк М.М. Відповідальність у міжнародному праві

Кваліфікаційна робота присвячена дослідженню міжнародно-правової відповідальності за кібероперації в умовах сучасних збройних конфліктів. Кваліфікаційна робота здобувача другого (магістерського) рівня вищої освіти містить три розділи, дев'ять підрозділів; її загальний обсяг становить 100 сторінок, у тому числі список використаних джерел, який налічує 90 найменувань.

Об'єктом дослідження є міжнародні правовідносини, що виникають у сфері здійснення кібероперацій під час міжнародних та неміжнародних збройних конфліктів.

Предметом дослідження є міжнародно-правові механізми регулювання та відповідальності за кібероперації в умовах сучасних міжнародних конфліктів.

Метою кваліфікаційної роботи є комплексне дослідження міжнародно-правових засад регулювання кібероперацій, особливостей міжнародно-правової відповідальності за їх здійснення, а також формування висновків і пропозицій щодо вдосконалення міжнародного гуманітарного права у сфері кібербезпеки.

Методологічну основу кваліфікаційної роботи становлять загальнонаукові та спеціально-юридичні методи пізнання. Діалектичний метод використано для дослідження розвитку міжнародно-правового регулювання кібероперацій та трансформації міжнародної безпеки в умовах цифровізації (розділи 1–3). Системний і структурно-функціональний методи дали змогу дослідити поняття, ознаки, види кібероперацій, підстави міжнародно-правової відповідальності та механізми міжнародного реагування у сфері кібербезпеки (розділи 1–3). Порівняльно-правовий метод застосовано для зіставлення міжнародних підходів до кваліфікації кібероперацій, визначення міжнародно-правової відповідальності держав та індивідуальної кримінальної відповідальності за кіберзлочини (розділи 1–3). Методи аналізу, синтезу, узагальнення, індукції, дедукції та прогнозування використано для формування висновків і пропозицій щодо вдосконалення міжнародного гуманітарного права у сфері кібероперацій (розділи 2–3).

У кваліфікаційній роботі досліджено поняття та сутність кібероперацій у міжнародному гуманітарному праві. Визначено особливості міжнародно-правової кваліфікації кібероперацій як форми застосування сили або збройного нападу. Проаналізовано джерела міжнародного гуманітарного права, що регулюють діяльність держав у кіберпросторі.

У роботі охарактеризовано підстави міжнародно-правової відповідальності держав за здійснення кібероперацій, визначено форми та види міжнародно-правової відповідальності, а також проаналізовано проблеми притягнення держав і фізичних осіб до відповідальності за міжнародно-протиправні дії у кіберпросторі.

У кваліфікаційній роботі досліджено сучасні міжнародні ініціативи та практику регулювання кібероперацій в умовах збройних конфліктів. Проаналізовано проблеми вдосконалення міжнародного гуманітарного права у сфері кібербезпеки, а також практику кібероперацій у російсько-українській війні та проблеми міжнародно-правового реагування на сучасні кіберзагрози.

Практичне значення отриманих результатів кваліфікаційної роботи полягає у

тому, що сформульовані в ній положення та висновки можуть бути використані:

1. у науково-дослідній сфері – для подальших досліджень міжнародно-правових проблем кібербезпеки та міжнародної відповідальності за кібероперації;
2. у правозастосовній діяльності – при вдосконаленні механізмів міжнародного реагування на кібератаки та розвитку національної системи кібербезпеки;
3. у сфері вищої освіти – під час викладання навчальних дисциплін «Міжнародне право», «Міжнародне гуманітарне право», «Правове регулювання кібербезпеки», «Міжнародна безпека».

Ключові слова: кібероперації, міжнародне гуманітарне право, міжнародно-правова відповідальність, кібербезпека, міжнародна безпека, кібератака, міжнародний збройний конфлікт, кіберпростір, критична інфраструктура, міжнародне право, міжнародні організації, міжнародні злочини, цифрова безпека, атрибуція кібератак.

Annotation

Ivaniuk M.M. Responsibility in International Law

The qualification thesis is devoted to the study of international legal responsibility for cyber operations in the context of modern armed conflicts. The qualification thesis for obtaining the second (Master's) level of higher education consists of three chapters and nine subsections; its total volume is 100 pages, including the list of references containing 90 sources.

The object of the research is international legal relations arising in the field of cyber operations during international and non-international armed conflicts.

The subject of the research is international legal mechanisms of regulation and responsibility for cyber operations in the context of modern international conflicts.

The purpose of the qualification thesis is a comprehensive study of the international legal foundations of cyber operations regulation, the peculiarities of international legal responsibility for their conduct, as well as the development of conclusions and proposals for improving international humanitarian law in the field of cybersecurity.

The methodological basis of the qualification thesis consists of general scientific and special legal methods of cognition. The dialectical method was used to study the development of international legal regulation of cyber operations and the transformation of international security in the context of digitalization (chapters 1–3). Systematic and structural-functional methods made it possible to examine the concepts, features, and types of cyber operations, the grounds for international legal responsibility, and international response mechanisms in the field of cybersecurity (chapters 1–3). The comparative legal method was applied to compare international approaches to the qualification of cyber operations, the determination of international legal responsibility of states, and individual criminal responsibility for cybercrimes (chapters 1–3). Methods of analysis, synthesis, generalization, induction, deduction, and forecasting were used to formulate conclusions and proposals for improving international humanitarian law in the field of cyber operations (chapters 2–3).

The qualification thesis examines the concept and essence of cyber operations in international humanitarian law. The peculiarities of the international legal qualification of

cyber operations as a form of the use of force or armed attack are determined. The sources of international humanitarian law regulating state activities in cyberspace are analyzed.

The thesis characterizes the grounds for international legal responsibility of states for conducting cyber operations, identifies the forms and types of international legal responsibility, and analyzes the problems of bringing states and individuals to responsibility for internationally wrongful acts in cyberspace.

The qualification thesis examines modern international initiatives and practices of regulating cyber operations in the context of armed conflicts. The problems of improving international humanitarian law in the field of cybersecurity are analyzed, as well as the practice of cyber operations in the Russian-Ukrainian war and the problems of international legal response to modern cyber threats.

The practical significance of the obtained results lies in the possibility of their use:

1. in scientific research activities – for further studies of international legal problems of cybersecurity and international responsibility for cyber operations;
2. in law enforcement activities – in improving mechanisms of international response to cyberattacks and developing the national cybersecurity system;
3. in higher education – during the teaching of the disciplines “International Law”, “International Humanitarian Law”, “Legal Regulation of Cybersecurity”, and “International Security”.

Keywords: cyber operations, international humanitarian law, international legal responsibility, cybersecurity, international security, cyberattack, international armed conflict, cyberspace, critical infrastructure, international law, international organizations, international crimes, digital security, attribution of cyberattacks.

ЗМІСТ КВАЛІФІКАЦІЙНОЇ РОБОТИ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АЕС – атомна електростанція

ЄС – Європейський Союз

КК – Кримінальний

кодекс

КПК – Кримінальний процесуальний

кодекс МВС – Міністерство

внутрішніх справ

МК – Митний кодекс

СІЗО – слідчий ізолятор

США – Сполучені штати Америки

УБОЗ – Управління по боротьбі з організованою

злочинністю УРСР – Українська Радянська

Соціалістична Республіка

ФРН – Федеративна Республіка Німеччина

ВСТУП

В умовах розвитку міжнародних відносин відбувається якісна зміна характеру взаємодії держав, що зумовлена стрімким впровадженням цифрових технологій у всі сфери суспільного життя. Кіберпростір поступово трансформується у самостійну сферу реалізації державної політики, включаючи сферу безпеки та оборони. У цьому контексті кібероперації набувають ознак інструменту, здатного впливати на хід міжнародних процесів нарівні з традиційними засобами збройного протистояння.

Використання кібероперацій у межах збройних конфліктів актуалізує питання їх правової природи та місця в системі міжнародного гуманітарного права. На відміну від класичних форм застосування сили, кібероперації характеризуються відсутністю чітко визначених територіальних меж, складністю ідентифікації суб’єкта їх здійснення та високим рівнем латентності.

Актуальність дослідження зумовлюється тим, що міжнародно-правове регулювання кібероперацій перебуває на стадії становлення і не забезпечує достатнього рівня правової визначеності. Наявні норми міжнародного гуманітарного права лише частково адаптовані до нових форм ведення конфліктів, що проявляється у відсутності єдиного підходу до визначення критеріїв збройного нападу у кіберпросторі, а також у неоднозначності підстав притягнення до міжнародно-правової відповідальності.

Практичний вимір цієї проблематики особливо чітко простежується в умовах сучасних збройних конфліктів, де кібероперації використовуються як елемент комплексного впливу на державу – від порушення функціонування

критичної інфраструктури до інформаційного впливу. Такі дії демонструють, що традиційні підходи до правового регулювання не повною мірою відповідають новим викликам, що виникають у сфері міжнародної безпеки.

Незважаючи на наявність значної кількості наукових досліджень, присвячених аспектам кібербезпеки та міжнародного права, питання міжнародно-правової відповідальності за кібероперації не отримало комплексного і системного висвітлення. Більшість наукових праць зосереджена на елементах проблеми, що обумовлює необхідність її цілісного аналізу з урахуванням сучасної практики та тенденцій розвитку міжнародного права.

Метою кваліфікаційної роботи є формування цілісного уявлення про правову природу кібероперацій у контексті міжнародного гуманітарного права та визначення ефективних механізмів міжнародно-правової відповідальності за їх здійснення.

Для досягнення поставленої мети сформульовано такі завдання:

1) визначити змістовні характеристики кібероперацій як явища міжнародно-правової дійсності;
2) встановити особливості нормативного регулювання кібероперацій у системі міжнародного гуманітарного права;
3) з’ясувати підходи до кваліфікації кібероперацій як збройного нападу;
4) визначити юридичні підстави відповідальності держав за здійснення кібероперацій;
5) окреслити форми реалізації міжнародно-правової відповідальності;
6) дослідити можливості притягнення фізичних осіб до міжнародної кримінальної відповідальності;
7) виявити проблемні аспекти встановлення відповідальності у кіберпросторі;
8) сформулювати напрями вдосконалення міжнародно-правового регулювання у цій сфері.

Об’єктом дослідження є суспільні відносини, що виникають у процесі здійснення кібероперацій у межах міжнародних збройних конфліктів.

Предметом дослідження є норми міжнародного гуманітарного права, доктринальні підходи та практика їх застосування у сфері регулювання кібероперацій і притягнення до відповідальності за їх здійснення.

Методологічна основа дослідження сформована із використанням комплексу взаємопов’язаних методів. Системний підхід забезпечив розгляд правового регулювання кібероперацій як цілісного явища; формально-юридичний метод застосовано для аналізу змісту правових норм; порівняльно-правовий метод дозволив виявити особливості підходів різних правових систем; логічний метод використано для узагальнення отриманих результатів та формулювання висновків.

Теоретичну основу становлять сучасні наукові розробки у сфері міжнародного права та кіберправа. Нормативну базу дослідження формують міжнародні договори, звичаєві норми, акти міжнародних організацій та практика їх застосування.

Практичне значення отриманих результатів полягає у можливості використання сформульованих висновків і пропозицій для вдосконалення правового регулювання кібероперацій, а також у навчальному процесі та наукових дослідженнях.

Структура кваліфікаційної роботи визначається логікою дослідження і складається зі вступу, трьох розділів, висновків та списку використаних джерел.

Апробацію результатів кваліфікаційної роботи реалізовано шляхом участі у IV Всеукраїнській науково-практичній конференції «Конституція Україн: стан, перспективи та механізм реалізації» на тему: «Відповідальність держав у кіберпросторі: міжнародно-правові підстави, форми та проблеми реалізації»

РОЗДІЛ 1. ТЕОРЕТИКО – ПРАВОВІ ЗАСАДИ КІБЕРОПЕРАЦІЙ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ ПРАВІ

1.1. Поняття та сутність кібероперацій

Теперешній етап розвитку міжнародних відносин характеризується суттєвими трансформаціями у сфері безпеки, що обумовлені стрімким розвитком інформаційно-комунікаційних технологій та формуванням кіберпростору як самостійного середовища взаємодії держав. У цих умовах кібероперації поступово набувають значення одного з ключових інструментів реалізації державної політики, у військовій та безпековій сферах. Їх застосування виходить за межі традиційних уявлень про використання сили, що зумовлює необхідність переосмислення існуючих підходів до їх правового регулювання в межах міжнародного гуманітарного права.

На данному етапі міжнародне право не містить універсального визначення поняття «кібероперація», що обумовлює існування різноманітних підходів до його тлумачення. Це пояснюється історичною обумовленістю розвитку міжнародно-правових норм, які формувалися у період, коли кіберпростір не відігравав значної ролі у міжнародних відносинах. У зв’язку з цим ключове значення у визначенні сутності кібероперацій мають доктринальні джерела та експертні напрацювання, серед яких особливе місце займає Талліннський посібник 2.0, що пропонує розглядати кібероперації як дії, що здійснюються через кіберпростір із використанням інформаційно-комунікаційних технологій з метою досягнення визначеного ефекту [16].

Сутність кібероперацій проявляється у використанні інформаційних технологій як засобу впливу, що дозволяє досягати стратегічних цілей без застосування традиційної збройної сили. Це означає, що кібероперації можуть виступати альтернативною формою реалізації державного примусу, що доповнює класичні механізми застосування сили. При цьому їх наслідки можуть бути співмірними з наслідками збройного нападу, у випадках, коли

вони призводять до порушення функціонування критичної інфраструктури або створюють загрозу життю та здоров'ю людей [14].

Особливістю кібероперацій є їх нематеріальний характер, що відрізняє їх від традиційних військових дій. У більшості випадків вони не супроводжуються фізичним руйнуванням об'єктів, однак можуть мати значний вплив на функціонування держави. Наприклад, втручання у роботу енергетичних систем або фінансових інституцій може призвести до масштабних економічних та соціальних наслідків без застосування фізичної сили [25]. Це, у свою чергу, ускладнює оцінку шкоди, завданої внаслідок таких операцій, та визначення її співмірності.

Кібероперації також характеризуються транснаціональністю, оскільки кіберпростір не має чітко визначених територіальних меж. Це дозволяє здійснювати вплив на об'єкти, розташовані в різних державах, без фактичного перетину державних кордонів. Така специфіка ставить під сумнів застосування традиційних принципів міжнародного права, принципу територіального суверенітету, який є одним із фундаментальних у системі міжнародних відносин.

Використання сучасних технологій дозволяє приховувати джерело атаки, що значно ускладнює процес атрибуції. У міжнародному праві атрибуція має вирішальне значення для притягнення держави до відповідальності, оскільки відповідальність настає лише у разі доведення зв'язку між діями та конкретною державою [7]. Кібероперації відзначаються високим рівнем універсальності, оскільки можуть використовуватися для досягнення різноманітних цілей, включаючи збір інформації, порушення функціонування систем, вплив на інформаційні процеси або забезпечення кіберзахисту. Вони часто розглядаються як елемент гібридної війни, що поєднує різні форми впливу, включаючи інформаційні, економічні та військові заходи. Їх використання у поєднанні з іншими інструментами дозволяє досягати значного ефекту без формального порушення міжнародно-правових

норм, що ускладнює їх правову оцінку та реагування з боку міжнародної спільноти [28].

На відміну від традиційних форм ведення війни, де основними суб'єктами виступають держави, у кіберпросторі значну роль відіграють також недержавні актори, включаючи хакерські угруповання, приватні компанії та осіб. Це ускладнює застосування норм міжнародного права, оскільки вони переважно орієнтовані на регулювання діяльності держав.

У розгляді питання міжнародного гуманітарного права ключовим є питання про те, чи можуть кібероперації бути кваліфіковані як застосування сили або збройний напад. Відповідно до Статуту Організації Об'єднаних Націй, державам забороняється застосування сили у міжнародних відносинах, за винятком випадків самооборони або санкцій Ради Безпеки [1].

Згідно з підходом, запропонованим у Талліннському посібнику, вирішальним критерієм є наслідки кібероперації. Якщо вони є співмірними з наслідками традиційного збройного нападу, така операція може розглядатися як застосування сили [16]. Це означає, що кібероперації можуть підпадати під дію норм міжнародного гуманітарного права, якщо вони досягають певного рівня інтенсивності. Розвиток зазначеного підходу вимагає врахування положень основних міжнародно-правових актів, що визначають рамки застосування сили у міжнародних відносинах. У сучасній доктрині міжнародного права підкреслюється, що ключовим критерієм для кваліфікації дій як застосування сили є не форма їх здійснення, а характер і масштаб наслідків [18; 19]. У цьому контексті кібероперації можуть розглядатися як форма застосування сили у разі, якщо їх вплив призводить до суттєвих порушень функціонування держави, її інфраструктури або створює загрозу життю та здоров'ю населення.

Зазначений підхід знаходить підтвердження і у практиці міжнародних судових органів, де неодноразово наголошувалося на пріоритетності оцінки фактичних наслідків дій [51]. Це дозволяє поширювати існуючі правові підходи на нові явища, кібероперації, навіть за відсутності їх прямого

нормативного закріплення у міжнародному праві. У межах міжнародного гуманітарного права важливим є питання визначення статусу кібероперацій як засобів або методів ведення війни. Традиційно засоби ведення війни охоплюють зброю та інші інструменти, що використовуються для ураження противника, тоді як методи визначають способи їх застосування. У кіберпросторі ці категорії тісно переплітаються, оскільки програмні засоби можуть одночасно виконувати обидві функції [23].

Принцип пропорційності, який вимагає, щоб шкода, завдана цивільним об’єктам, не перевищувала очікувану військову перевагу [3]. У випадку кібероперацій прогнозування наслідків є особливо складним, оскільки навіть незначне втручання може спричинити масштабні збої у функціонуванні систем. Це пов’язано з високим рівнем взаємозалежності сучасної інфраструктури, де порушення в одному секторі можуть призвести до ланцюгової реакції в інших.

Принцип військової необхідності також набуває специфічного змісту у кіберпросторі. Він передбачає, що будь-які дії повинні бути спрямовані на досягнення законної військової мети [2]. У традиційних конфліктах захист цивільного населення забезпечується шляхом обмеження засобів і методів ведення війни [2]. У кіберпросторі такі механізми є менш ефективними через складність контролю над поширенням шкідливого програмного забезпечення. Використані інструменти можуть виходити за межі запланованої цілі та впливати на широке коло об’єктів, включаючи ті, що не мають жодного відношення до конфлікту [25].

Встановлення суб’єкта, відповідального за здійснення певної дії, є ключовим для притягнення до міжнародно-правової відповідальності. У кіберпросторі це завдання ускладнюється використанням технологій, що дозволяють приховувати джерело атаки або створювати хибні сліди.

Кібероперації також змінюють уявлення про просторові межі збройного конфлікту. На відміну від традиційних бойових дій, які прив’язані до конкретної території, кібероперації можуть здійснюватися дистанційно,

охоплюючи об’єкти, розташовані у різних частинах світу. Це створює нові виклики для застосування принципу територіального суверенітету та визначення юрисдикції держав.

На відміну від класичних збройних конфліктів, де основними суб’єктами виступають держави, у кібероперaціях значну роль можуть відігравати приватні компанії, хакерські групи та іншіособи [17]. Це ускладнює застосування міжнародного гуманітарного права, оскільки його норми переважно спрямовані на регулювання діяльності держав. Їх використання дозволяє досягати значного ефекту без прямого застосування збройної сили, що змінює характер міжнародного протистояння та підвищує роль нематеріальних факторів.

Відсутність чітких норм, які б безпосередньо регулювали кібероперації, зумовлює необхідність розвитку правової доктрини та вироблення єдиних підходів до їх оцінки. Дослідження кібероперацій у контексті міжнародного гуманітарного права потребує звернення до теоретичних підходів, сформованих у навчальній та науковій літературі з кібербезпеки. У підручниках підкреслюється, що кіберпростір є складною соціотехнічною системою, яка поєднує технічні засоби, програмне забезпечення та людський фактор.

Аналіз технічних характеристик кібероперацій має суттєве значення для їх розуміння. Вони відрізняються високою швидкістю здійснення та можливістю прихованого впливу. Це дозволяє реалізовувати дії без негайного виявлення. Кібероперації також тісно пов’язані з функціонуванням національних систем безпеки. У законодавстві України кібербезпека визначається як складова національної безпеки.

1.2. Правова природа кібероперацій у системі міжнародного гуманітарного права

Осмислення правової природи кібероперацій потребує звернення до їх функціонального значення у сучасних міжнародних відносинах. Їх

застосування охоплює політичні, економічні та інформаційні процеси, що свідчить про універсальний характер цього явища. Кібероперації можуть виступати засобом впливу на державні інститути, порушення стабільності функціонування суспільних систем та створення умов для досягнення переваги без прямого застосування сили. Вони дозволяють здійснювати тиск у формах, які складно однозначно кваліфікувати у межах міжнародного права. У навчальній літературі підкреслюється, що функціонування кіберпростору як багаторівневої системи створює можливості для різних форм впливу залежно від обраної цілі [70, с. 118–120].

Кібероперації можуть комбінуватися з іншими формами впливу, що підсилює їх ефективність. У сучасних умовах вони зазвичай поєднуються з інформаційними кампаніями, економічними заходами та політичними рішеннями. У підручниках з кібербезпеки зазначається, що поєднання технічних і соціальних факторів визначає результат впливу [71, с. 52–54]. Це підкреслює необхідність врахування не лише технічних характеристик, але й поведінкових аспектів. Правова оцінка кібероперацій у таких умовах не може обмежуватися аналізом способів їх здійснення. Вона повинна враховувати цілі, які переслідуються, та наслідки, що виникають у результаті реалізації таких дій. Сукупність цих факторів визначає їх місце у системі міжнародного гуманітарного права.

Розвиток цифрових технологій призвів до формування складних мережевих структур, у яких різні елементи тісно пов’язані між собою. Це створює додаткові ризики, пов’язані з використанням кібероперацій. Прогнозування їх наслідків стає складнішим через високий рівень взаємозалежності інфраструктури.

Втручання у фінансові системи або логістичні мережі може призвести до значних економічних втрат. Значна частина критичної інфраструктури перебуває у власності приватних компаній. Це ускладнює координацію дій у разі виникнення загроз. Виникає необхідність розвитку механізмів взаємодії між державними та недержавними суб’єктами. У навчальній літературі

підкреслюється, що кібербезпека є спільною відповідальністю різних акторів [58, с. 60–62].

Кібероперації можуть бути спрямовані на підрив довіри до інформаційних систем. Це має довгострокові наслідки для функціонування держави. Втрата довіри може призвести до дестабілізації соціальних і економічних процесів.

Застосування автоматизованих систем та штучного інтелекту суттєво змінює характер кібероперацій. Воно дозволяє підвищити їх швидкість та ефективність. Кібероперації можуть використовуватися як інструмент асиметричного впливу. Держави з обмеженими ресурсами отримують можливість протистояти більш потужним супротивникам. Це змінює баланс сил у міжнародних відносинах [20]. Ефективна протидія кіберзагрозам потребує координації дій держав. Вона включає обмін інформацією та розробку спільних стандартів [8].

Практика реалізації кібероперацій свідчить про їх поступову інституціоналізацію. Держави створюють спеціалізовані структури для реагування на кіберінциденти [59]. Кібероперації дедалі частіше мають багатофазний характер. Вони включають проникнення, закріплення та розширення впливу [85]. Аналіз кіберінцидентів демонструє зростання їх складності та масштабів [88]. Це підтверджує тенденцію до системного використання кібероперацій. У сучасних конфліктах вони доповнюють традиційні військові дії [89].

Розвиток кіберпростору супроводжується активною участю наукових та аналітичних центрів. Їх діяльність сприяє формуванню сучасних підходів до кібербезпеки [63; 65]. Нові технології, штучний інтелект та великі дані, розширюють можливості кібероперацій [67; 68]. Кіберзагрози набувають глобального характеру. Вони можуть здійснюватися з використанням інфраструктури різних держав [61]. Це створює труднощі для визначення юрисдикції. У стратегічних документах визначаються пріоритети розвитку

кібербезпеки [60]. Підготовка фахівців повинна враховувати як технічні, так і правові аспекти [70, с. 135].

Кібероперації поступово трансформуються у невід'ємний елемент сучасної архітектури безпеки, що впливає на спосіб формування та реалізації державної політики. Їх використання дозволяє досягати стратегічних результатів без прямого зіткнення сторін, що змінює уявлення про природу конфлікту. Вони можуть виконувати допоміжну функцію або виступати самостійним інструментом впливу. Це створює ситуацію, коли межа між мирним і воєнним станом стає менш чіткою. У навчальній літературі підкреслюється, що кіберпростір формує новий тип взаємодії, у якому відсутність фізичного контакту не означає відсутності впливу [71, с. 88–90].

Держави все частіше здійснюють дії, спрямовані на попередження потенційних загроз. Відсутність чітко визначених норм ускладнює оцінку таких дій. У підручниках зазначається, що кібербезпека передбачає не лише реагування, але й активні дії щодо запобігання ризикам [58, с. 67–69].

На відміну від традиційних військових дій, вони можуть здійснюватися миттєво або розтягуватися у часі. Це ускладнює їх ідентифікацію та реагування на них. У навчальних матеріалах підкреслюється, що швидкість є однією з ключових характеристик кіберпростору [70, с. 140–142]. Це означає, що рішення повинні прийматися у максимально короткі терміни. Така комбінація швидкості та відкладеного ефекту створює додаткові труднощі для правової оцінки. Вона також впливає на ефективність механізмів реагування.

Встановлення суб'єкта, відповідального за здійснення втручання, є ключовим для притягнення до відповідальності. Однак у кіберпросторі це завдання ускладнюється використанням технологій маскування. Атаки можуть здійснюватися через мережі різних держав, що ускладнює їх відстеження. У наукових дослідженнях підкреслюється, що проблема атрибуції є однією з центральних у сфері кібербезпеки [61]. Вона безпосередньо впливає на можливість застосування міжнародного права.

Відсутність чітких доказів обмежує можливості реагування. Це створює передумови для безкарності.

Кібероперації також змінюють підходи до захисту об’єктів у межах міжнародного гуманітарного права. У традиційних конфліктах існує чітке розмежування між військовими та цивільними об’єктами. У кіберпросторі така диференціація є значно складнішою. Багато систем мають подвійне призначення. Вони використовуються як у цивільних, так і у військових цілях. Це ускладнює визначення їх правового статусу. У підручниках зазначається, що інтеграція систем є однією з ключових характеристик сучасного кіберпростору [75, с. 80–82]. Це означає, що вплив на один об’єкт може зачіпати інші.

Оцінка шкоди, завданої такими діями, є складною через їх нематеріальний характер. Наслідки можуть проявлятися у вигляді порушення функціонування систем, а не їх фізичного знищення. Це ускладнює визначення їх співмірності. У навчальній літературі підкреслюється, що оцінка ризиків у кіберпросторі має ймовірнісний характер [58, с. 73–75]. Це означає, що точне прогнозування наслідків є практично неможливим. Виникає необхідність врахування непрямих ефектів. Це включає вплив на суміжні системи.

Розвиток кібероперацій також пов’язаний із зміною ролі інформації у сучасному суспільстві. Вона стає ключовим ресурсом, від якого залежить функціонування держави. Втручання у інформаційні потоки може мати стратегічні наслідки. Це підсилює значення кібероперацій як інструменту впливу. У контексті розвитку міжнародного співробітництва важливим є формування спільних підходів до регулювання кіберпростору. Держави поступово усвідомлюють необхідність координації своїх дій. Це включає обмін інформацією та розробку спільних стандартів. У міжнародних ініціативах підкреслюється важливість довіри між державами [8].. Це ускладнює досягнення консенсусу.

Розвиток освітніх та наукових програм у сфері кібербезпеки безпосередньо пов’язаний із формуванням аналітичного потенціалу держави. Йдеться не лише про підготовку технічних спеціалістів, але і про створення фахівців, здатних оцінювати кібероперації у ширшому правовому та безпековому контексті. Відповідно, освітні програми мають орієнтуватися на розвиток навичок критичного мислення та комплексного аналізу. Це дозволяє не лише виявляти кіберзагрози, але й прогнозувати їх можливі наслідки.

Паралельно із розвитком освіти відбувається посилення ролі наукових досліджень, спрямованих на вивчення кібероперацій. Наукові установи та аналітичні центри формують теоретичну базу, яка дозволяє систематизувати знання про сучасні загрози. Вони також розробляють методики оцінки ризиків та прогнозування можливих сценаріїв. Це створює підґрунтя для більш обґрунтованих управлінських рішень. Воно об’єднує фахівців з різних галузей, що сприяє обміну знаннями та досвідом. Така взаємодія дозволяє виробляти узгоджені підходи до аналізу кібероперацій. Вона сприяє уніфікації термінології та методології досліджень. У підручниках підкреслюється, що міждисциплінарність є ключовою умовою розвитку кібербезпеки як науки [70, с. 151].

Розвиток професійного середовища у сфері кібербезпеки також впливає на формування практики реагування на кібероперації на міжнародному рівні. Взаємодія експертів, державних органів і наукових установ сприяє виробленню узгоджених підходів до оцінки загроз. Це дозволяє підвищити ефективність обміну інформацією та координації дій у разі виникнення інцидентів. Жодна держава не може ефективно протидіяти кіберзагрозам ізольовано. Формується тенденція до створення спільних платформ для співробітництва. У їх межах здійснюється аналіз інцидентів, розробка рекомендацій та обмін досвідом.

Швидкість технологічних змін випереджає темпи правового регулювання, що створює розрив між практикою та правом. У цих умовах важливого значення набуває гнучкість правових механізмів. Вони повинні

бути здатними адаптуватися до нових викликів без втрати ефективності. У наукових дослідженнях підкреслюється необхідність поєднання стабільності правових норм із їх динамічним розвитком. Це дозволяє забезпечити баланс між передбачуваністю та адаптивністю. Особливу роль відіграють доктринальні підходи, які заповнюють прогалини у нормативному регулюванні. Вони формують основу для розвитку міжнародного права.

Традиційно безпека асоціювалася з фізичним захистом території та ресурсів. У цифрову епоху вона набуває багатовимірного характеру. Захист інформаційних систем стає не менш важливим, ніж захист матеріальних об’єктів. Це змінює підходи до формування державної політики. Кібербезпека інтегрується у всі сфери діяльності держави. Вона охоплює економіку, управління, оборону та соціальну сферу. Така інтеграція потребує комплексного підходу до аналізу загроз.

Правова природа кібероперацій формується під впливом глибоких трансформацій у сфері міжнародних відносин та розвитку цифрових технологій. Їх специфіка полягає у нематеріальному характері, багаторівневій структурі та здатності впливати на різні сфери функціонування держави. На відміну від традиційних форм застосування сили, кібероперації можуть здійснюватися без фізичного контакту, але при цьому мати значні наслідки. Це ускладнює їх правову кваліфікацію та вимагає адаптації існуючих норм міжнародного гуманітарного права.

Аналіз показує, що ключовим критерієм для оцінки кібероперацій є їх наслідки, а не форма здійснення. У разі досягнення рівня інтенсивності, співмірного з традиційними формами застосування сили, вони можуть підпадати під дію відповідних норм міжнародного права. Особливу складність становить застосування базових принципів міжнародного гуманітарного права у кіберпросторі. Принципи розрізнення, пропорційності та військової необхідності потребують переосмислення з урахуванням специфіки цифрового середовища. Високий рівень взаємозалежності систем ускладнює прогнозування наслідків та визначення меж допустимого впливу.

Отже, кібероперації у сучасних умовах слід розглядати як самостійний та багатовимірний феномен, що поєднує технічні, правові та політичні складові. Їх специфіка полягає у здатності впливати на функціонування держави без застосування традиційної збройної сили, що змінює підходи до розуміння безпеки та конфлікту. Визначальним для їх правової оцінки виступає не форма реалізації, а характер і масштаб наслідків, які можуть бути співмірними з наслідками класичних військових дій. Відсутність чітко сформульованих міжнародно-правових норм щодо кібероперацій створює ситуацію нормативної невизначеності, що ускладнює їх кваліфікацію та притягнення до відповідальності. Застосування принципів міжнародного гуманітарного права у кіберпросторі потребує адаптації з урахуванням високого рівня взаємозалежності систем та складності прогнозування наслідків.

1.3. Проблеми застосування норм міжнародного гуманітарного права до кібероперацій

Застосування норм міжнародного гуманітарного права до кібероперацій ускладнюється відсутністю чітких критеріїв їх правової кваліфікації. Норми формувалися для фізичного середовища, тоді як кібероперації здійснюються без матеріального впливу. Навіть за наявності значних наслідків такі дії не завжди однозначно підпадають під категорію застосування сили. У доктрині визнається можливість застосування чинних норм, однак за умови їх адаптації [16]. Аналітичні дослідження підтверджують зростання ролі кібероперацій у сучасних конфліктах [61].

Проблемним залишається визначення моменту, коли кібероперація досягає рівня збройного нападу. Традиційні критерії пов’язані з фізичними руйнуваннями, тоді як кібероперації часто спричиняють функціональні порушення. Такі наслідки можуть бути масштабними, але складними для вимірювання. Підхід, заснований на оцінці інтенсивності наслідків,

застосовується, але не є уніфікованим [18]. Практика кіберінцидентів демонструє значну різницю у підходах до їх оцінки [88]. Це створює ризик довільного тлумачення.

Застосування принципу розрізнення у кіберпросторі ускладнюється подвійним призначенням більшості систем. Одна інфраструктура одночасно забезпечує цивільні та військові функції. Вплив на неї не може бути локалізований. Це підвищує ризик завдання шкоди цивільним об’єктам. Інтегрованість мереж ускладнює відмежування цілей [70, с. 162–164]. Дані аналітичних звітів підтверджують зростання атак на критичну інфраструктуру [80].

Принцип пропорційності також втрачає однозначність через нематеріальний характер шкоди. Наслідки кібероперацій часто проявляються у збої систем або втраті доступу до інформації. Їх масштаб складно оцінити до моменту реалізації. Прогнозування має ймовірнісний характер [58, с. 73–75]. Дослідження підтверджують складність оцінки довгострокових ефектів [26].

Проблема атрибуції є ключовою для застосування міжнародно-правової відповідальності. Встановлення суб’єкта кібероперації ускладнюється технічними можливостями маскування. Використання інфраструктури інших держав ускладнює ідентифікацію джерела. Навіть значні інциденти не завжди можуть бути однозначно пов’язані з конкретною державою [7]. Це обмежує застосування механізмів відповідальності. Аналітичні дослідження визначають атрибуцію як основну проблему правового реагування [61].

Правовий статус даних як об’єкта захисту залишається невизначеним. Втручання у дані може мати наслідки, співставні з фізичним руйнуванням. У дослідженнях зазначається необхідність розширення підходів до визначення шкоди [14]. Відсутність чітких критеріїв ускладнює кваліфікацію таких дій. Участь недержавних акторів у кібероперaціях ускладнює застосування норм міжнародного права. Значна частина атак здійснюється не державами, а групами або іншими особами. Міжнародне право орієнтоване на держави, що обмежує його ефективність у таких випадках. У підручниках підкреслюється

мультиакторний характер кіберпростору [71, с. 110–112]. Це вимагає перегляду підходів до правового регулювання.

Підходи до застосування міжнародного гуманітарного права у кіберпросторі пов’язані із необхідністю уточнення режиму юрисдикції держав. Кібероперації можуть здійснюватися з території однієї держави, використовуючи інфраструктуру іншої, та спрямовуватися проти третьої. Така багаторівнева структура ускладнює визначення того, яке право має застосовуватися. У міжнародних дослідженнях підкреслюється, що територіальний принцип у кіберпросторі втрачає свою однозначність [62]. Це створює ситуацію перетину юрисдикцій. Відсутність узгоджених правил призводить до конфліктів компетенцій.

Складність правового регулювання посилюється через швидкість еволюції технологій. З’являються нові інструменти, здатні автоматично адаптуватися до систем захисту. Використання штучного інтелекту дозволяє змінювати поведінку кібероперацій у реальному часі. За даними технологічних досліджень, такі системи здатні самостійно обирати найбільш ефективні способи впливу [67].

Для юридичної кваліфікації необхідно підтвердити як факт втручання, так і його наслідки. Однак цифрові сліди можуть бути змінені або знищені. У міжнародних дослідженнях зазначається, що збір доказів у кіберпросторі потребує спеціалізованих методів і технічних ресурсів [64]. Відсутність уніфікованих стандартів у цій сфері знижує ефективність розслідувань.

Значний вплив на застосування міжнародного гуманітарного права має також комерціалізація кіберпростору. Приватні компанії виступають власниками значної частини інфраструктури. Вони також розробляють технології, які можуть використовуватися у кіберопераціях. У дослідженнях підкреслюється, що взаємодія держав і приватного сектору стає необхідною умовою забезпечення кібербезпеки [87].

Кібероперації також впливають на трансформацію механізмів стримування у міжнародних відносинах. Традиційні моделі стримування

базувалися на демонстрації військової сили. У кіберпросторі така демонстрація є менш очевидною. Анонімність і складність атрибуції знижують ефективність класичних підходів. У сучасних дослідженнях зазначається, що кіберстримування потребує нових інструментів, включаючи дипломатичні та економічні заходи [63].

Різні держави використовують власні методики оцінки загроз. У міжнародних ініціативах підкреслюється необхідність розробки спільних стандартів [48]. Такі стандарти можуть включати класифікацію інцидентів та алгоритми реагування. Їх впровадження сприятиме підвищенню ефективності співробітництва.

Проблематика застосування міжнародного гуманітарного права до кібероперацій також пов’язана з необхідністю врахування людського фактора. Помилки операторів або недосконаліть систем можуть призводити до непередбачуваних наслідків. У дослідженнях підкреслюється, що людський фактор залишається одним із ключових елементів кібербезпеки [58, с. 90–92].

Використання кібероперацій у режимі постійної активності змінює логіку застосування міжнародного гуманітарного права, оскільки значна частина дій відбувається поза межами формально оголошених конфліктів. Такі дії можуть мати тривалий характер і спрямовуватися на підрив стабільності інформаційних систем, не досягаючи рівня відкритого протистояння. У міжнародних дослідженнях наголошується, що кіберпростір дедалі частіше використовується як середовище постійного стратегічного тиску [65]. Відсутність чіткої межі між миром і конфліктом призводить до правової невизначеності.

Фрагментованість міжнародного регулювання посилює зазначені труднощі, оскільки різні суб’єкти формують власні підходи до кібербезпеки. Наявність численних ініціатив і рекомендацій не забезпечує їх уніфікованого застосування. У наукових дослідженнях підкреслюється, що відсутність єдиної нормативної системи знижує ефективність міжнародного права у цій сфері [62]. Держави орієнтуються на власні пріоритети безпеки.

Особливу складність становить забезпечення захисту критичної інформаційної інфраструктури, яка функціонує як єдина взаємопов’язана система. Вплив на елемент може спричинити ланцюгову реакцію в інших секторах. За даними міжнародних аналітичних досліджень, такі системи залишаються одними з основних цілей кібероперацій [64]. Їх ураження може призвести до порушення функціонування держави в цілому.

Економічний вимір кібероперацій також потребує врахування, оскільки цифрові технології є основою сучасних фінансових систем. Втручання у їх функціонування може мати наслідки, що виходять за межі окремої держави. Міжнародні дослідження фіксують зростання впливу кіберзагроз на глобальні економічні процеси [50].

Політичний вплив через кібероперації формує ще один рівень складності, оскільки втручання у інформаційні процеси може змінювати внутрішню стабільність держав. Такі дії включають маніпулювання даними, поширення дезінформації та втручання у комунікаційні системи. Вони не супроводжуються фізичним насильством, але мають значні наслідки. У сучасних дослідженнях зазначається, що інформаційний компонент стає ключовим елементом кібероперацій [63].

Обмеженість механізмів примусу у міжнародному праві посилює зазначені проблеми, оскільки навіть встановлення порушення не гарантує ефективного реагування. Реалізація відповідальності залежить від політичної волі держав. У кіберпросторі ця залежність посилюється через складність доведення фактів. Міжнародні дослідження підкреслюють, що механізми стримування у цифровому середовищі залишаються недостатньо розвиненими [63].

Суттєвого значення набуває проблема співвідношення кібероперацій із нормами міжнародного права прав людини. Вплив на інформаційні системи може призводити до обмеження доступу до інформації, порушення приватності або блокування цифрових сервісів. Такі наслідки безпосередньо зачіпають права людини навіть за відсутності фізичного насильства. У

міжнародних дослідженнях підкреслюється, що цифровий простір став середовищем реалізації базових прав і свобод [48]. Виникає необхідність одночасного застосування різних правових режимів. Така ситуація ускладнює правову кваліфікацію дій. Відсутність чітких критеріїв співвідношення цих норм створює ризик їх вибіркового застосування.

Технологічна складність кібероперацій змінює підходи до їх аналізу, оскільки значна частина процесів відбувається автоматизовано. Використання складних алгоритмів і програмних засобів дозволяє здійснювати вплив без прямого втручання людини. Така автономність ускладнює визначення наміру та ступеня контролю. У наукових дослідженнях зазначається, що автоматизація підвищує ефективність кібероперацій, але водночас ускладнює їх правову оцінку [68]. Виникає питання відповідальності за дії систем, що функціонують автономно. Традиційні підходи до встановлення вини не враховують подібних ситуацій.

У кіберпросторі значну роль відіграють технічні протоколи та правила функціонування мереж. Вони визначають можливості як захисту, так і здійснення кібероперацій. У дослідженнях зазначається, що технічні стандарти фактично формують основу цифрового середовища [64].

Особливість кіберпростору полягає в тому, що його функціонування забезпечується не лише державами, але й приватними суб’єктами, міжнародними технічними організаціями, розробниками програмного забезпечення та операторами цифрової інфраструктури. Вони формують архітектуру мережі Інтернет, визначають механізми обміну даними, стандарти шифрування, автентифікації та маршрутизації інформації.

Технічний аспект кібероперацій має безпосередній вплив на питання застосування міжнародного гуманітарного права. Наприклад, встановлення факту втручання в інформаційну систему потребує проведення цифрової експертизи, аналізу мережевого трафіку, логів та інших електронних даних. Без належного технічного підтвердження практично неможливо здійснити атрибуцію кібероперації конкретній державі чи організованій групі. Проблема

атрибуції сьогодні визнається однією з ключових перешкод для ефективного механізму міжнародно-правової відповідальності у кіберпросторі [16].

Складність також полягає у тому, що сучасні кібероперації часто здійснюються із використанням проміжних серверів, бот-мереж, викрадених облікових записів та інфраструктури третіх держав. Коли джерело атаки технічно може знаходитися на території однієї держави, тоді як фактичний організатор перебуває в іншій юрисдикції. У міжнародному праві така ситуація породжує труднощі щодо встановлення контролю держави над відповідними діями, що є необхідним елементом для покладення міжнародно-правової відповідальності [7].

Швидкий розвиток цифрових технологій значно випереджає темпи формування міжнародно-правових норм. Більшість положень міжнародного гуманітарного права була створена ще до виникнення кіберпростору як окремої сфери конфлікту. Тому сучасна юридична доктрина змушена адаптовувати вже існуючі принципи до нових технологічних реалій. Йдеться насамперед про принципи розрізнення, пропорційності, військової необхідності та гуманності, які повинні застосовуватись і під час здійснення кібероперацій [14].

Особливої уваги потребує питання захисту критичної інфраструктури. У сучасних умовах енергетичні системи, транспортні мережі, банківський сектор, медичні заклади та системи зв’язку значною мірою залежать від цифрових технологій. Втручання в їхню роботу може спричинити наслідки, співмірні із застосуванням традиційних видів озброєння. Міжнародні організації дедалі частіше визнають необхідність формування спеціальних механізмів захисту цивільної цифрової інфраструктури під час збройних конфліктів [8].

Значний вплив на формування сучасного підходу до тлумачення міжнародного права у кіберпросторі має Tallinn Manual 2.0, у якому систематизовано підходи до визначення кібероперацій, критеріїв збройного нападу, державної відповідальності та застосування норм міжнародного

гуманітарного права у цифровому середовищі [16]. Хоча цей документ не має обов’язкової юридичної сили, він став важливим орієнтиром для держав, міжнародних організацій та науковців.

РОЗДІЛ 2. МІЖНАРОДНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРОПЕРАЦІЇ

2.1. Підстави відповідальності держав

Розвиток інформаційних технологій суттєво змінив характер сучасних міжнародних конфліктів. Держави отримали можливість впливати на політичні, економічні та військові процеси інших країн без використання традиційних засобів ведення війни. Кібероперації сьогодні застосовуються для збору розвідувальної інформації, втручання у роботу державних систем, дестабілізації критичної інфраструктури та здійснення інформаційного впливу. У зв’язку з цим міжнародне право поступово адаптує механізми відповідальності держав до нових форм діяльності у цифровому середовищі.

Питання міжнародно-правової відповідальності держав у кіберпросторі ґрунтується на загальних принципах міжнародного права. Незважаючи на відсутність універсального міжнародного договору, який би окремо регулював кібероперації, відповідальність держав у цій сфері виникає на підставі вже існуючих норм міжнародного права [7]. Ключовим документом у цьому контексті є Проєкт статей про відповідальність держав за міжнародно-протиправні діяння, розроблений Комісією міжнародного права ООН у 2001 році. У ньому зазначається, що міжнародно-протиправним є будь-яке діяння держави, яке порушує її міжнародне зобов’язання та може бути віднесене до цієї держави [7].

Для виникнення міжнародно-правової відповідальності необхідна наявність двох основних елементів - порушення міжнародного зобов’язання та можливість атрибуції відповідних дій державі. Порушення міжнародного зобов’язання у кіберпросторі може проявлятися у різних формах. Насамперед йдеться про порушення принципу державного суверенітету. У сучасному

міжнародному праві суверенітет поширюється не лише на територію держави, а й на її інформаційну інфраструктуру, державні мережі, системи зв'язку та цифрові ресурси. Несанкціоноване втручання у роботу державних інформаційних систем може розглядатися як порушення суверенних прав держави [16].

Кібероперації також можуть порушувати принцип невтручання у внутрішні справи держав. Особливо це стосується ситуацій, коли кібератаки спрямовані на вплив на виборчі процеси, функціонування органів державної влади, фінансової системи або на дестабілізацію внутрішньої ситуації у державі. Такі дії розглядаються як форма зовнішнього впливу на політичну незалежність держави та суперечать основним принципам Статуту ООН [1].

Має значення заборона застосування сили, закріплена у статті 2 Статуту Організації Об'єднаних Націй [1]. Сучасна міжнародно-правова доктрина виходить із того, що певні кібероперації можуть бути прирівняні до застосування сили, якщо їх наслідки є співмірними із наслідками традиційного воєнного нападу. Йдеться про випадки, коли кібератака призводить до руйнування об'єктів, порушення роботи критичної інфраструктури, аварій на промислових підприємствах, транспортних катастроф або загибелі людей [18].

У Tallinn Manual 2.0 зазначається, що визначальним критерієм є не спосіб здійснення атаки, а масштаб та наслідки відповідної операції [16]. Якщо кібероперація спричиняє фізичні руйнування або створює серйозну загрозу безпеці держави, вона може кваліфікуватися як застосування сили у розумінні міжнародного права. У такому випадку держава-жертва отримує право на самооборону відповідно до статті 51 Статуту ООН [1].

На практиці найбільшу складність становить питання атрибуції кібероперацій. У традиційних міжнародних конфліктах визначення сторони, яка здійснила напад, зазвичай не викликає значних труднощів. У кіберпросторі ситуація є іншою. Сучасні технології дозволяють приховувати джерело атаки, використовувати сервери третіх держав, анонімні мережі, шкідливе програмне забезпечення та інші засоби маскування. Через це встановлення держави,

відповідальної за кібератаку, перетворюється на складний процес, що поєднує технічний, політичний та юридичний аспекти [17].

Держави нерідко використовують для здійснення кібероперацій недержавних суб'єктів - хакерські групи, приватних виконавців або напівофіційні організації. Формально такі особи можуть не належати до державного апарату, однак фактично діяти в інтересах держави або за її підтримки. У справі «Нікарагуа проти США» Суд зазначив, що для покладення відповідальності необхідно довести ефективний контроль держави над діями відповідних груп [51]. Цей критерій передбачає, що держава повинна не лише підтримувати певних осіб, а й здійснювати реальний контроль над їхньою діяльністю. У сфері кібероперацій застосування такого підходу є складним, оскільки держави переважно уникають прямого зв'язку з виконавцями атак.

Попри це, у сучасній міжнародній практиці дедалі частіше використовується політична атрибуція. Держави публічно покладають відповідальність за кібератаки на інші держави на підставі сукупності технічних доказів, даних розвідки та аналізу характеру атаки. Подібна практика активно застосовується державами-членами НАТО та Європейського Союзу [10]. Хоча такі заяви не завжди супроводжуються повним розкриттям доказів, вони формують міжнародну практику реагування на кіберінциденти.

Підставою міжнародно-правової відповідальності є невиконання державою обов'язку належної обачності. Суть цього принципу полягає у тому, що держава повинна вживати заходів для недопущення використання своєї території або інфраструктури для завдання шкоди іншим державам [16]. У кіберпросторі це означає обов'язок держави реагувати на діяльність хакерських груп, які використовують її мережі для здійснення кібератак.

Якщо держава знає про таку діяльність, але не вживає необхідних заходів для її припинення, це може розглядатися як порушення міжнародного права. Особливо актуальним це питання стало у зв'язку з поширенням

міжнародних хакерських угруповань, діяльність яких нерідко має транскордонний характер.

Проблема відповідальності держав за кібероперації особливо загострюється під час збройних конфліктів. Принцип розрізнення передбачає обов'язок відмежовувати військові цілі від цивільних об'єктів. У кіберпросторі це створює значні труднощі, оскільки цивільна та військова інфраструктура часто є взаємопов'язаними. Наприклад, одна й та сама телекомунікаційна мережа може використовуватися як цивільними установами, так і військовими структурами. Через це кібератака на військову систему може одночасно вплинути і на цивільне населення [14].

Принцип пропорційності забороняє здійснення атак, наслідки яких для цивільного населення будуть надмірними порівняно з очікуваною військовою перевагою [3]. У контексті кібероперацій це означає необхідність оцінки можливих наслідків втручання у роботу критичної інфраструктури. Наприклад, виведення з ладу енергетичної системи може призвести до припинення роботи лікарень, систем водопостачання та транспорту, що створює загрозу життю цивільного населення.

Міжнародно-правова відповідальність держав у кіберпросторі стала особливо актуальною після низки масштабних кібератак останніх років. Одним із найбільш відомих прикладів є атака вірусу NotPetya у 2017 році, яка спричинила значні збитки державним та приватним структурам у різних країнах світу. Низка держав офіційно поклала відповідальність за цю атаку на Російську Федерацію [88]. Під час російсько-української війни кібероперації стали складовою військових дій. Кібератаки здійснювалися проти енергетичної системи України, державних реєстрів, банківського сектору та телекомунікаційної інфраструктури. У багатьох випадках вони поєднувалися з ракетними ударами, що свідчить про використання кіберпростору як елемента сучасної війни. Відсутність спеціального міжнародного договору, складність атрибуції та політичний характер міжнародних відносин значно ускладнюють практичну реалізацію відповідальності. Більшість механізмів

реагування сьогодні мають політичний або санкційний характер. Держави дедалі частіше визнають застосовність норм міжнародного права до кібероперацій та необхідність дотримання міжнародно-правових зобов'язань у цифровому середовищі.

Кіберпростір ускладнив розуміння державної участі у протиправних діях. У багатьох випадках між замовником операції та її виконавцем існує декілька ланок - приватні структури, афілійовані групи, технічні посередники. Це дозволяє державам формально дистанціюватися від атак навіть тоді, коли операція відповідає їхнім політичним або військовим інтересам. Через це міжнародне право стикається з проблемою доведення не лише факту втручання, а й рівня причетності держави до конкретних дій.

Держава у кіберпросторі отримала можливість діяти непрямо. Якщо під час звичайного воєнного нападу можна встановити належність військової техніки, місце запуску ракети або участь конкретного підрозділу, то у цифровому середовищі між організатором атаки та її виконанням часто існує складна система посередників. Частину операцій виконують приватні компанії, частину - окремі хакерські групи, які формально не входять до структури державних органів.

На практиці це створює ситуацію, коли держава фактично користується результатами кібероперації, але водночас зберігає можливість заперечувати власну причетність. Наприклад, у діяльності багатьох російських хакерських угруповань простежується збіг між їхніми атаками та політичними або військовими інтересами Російської Федерації. Особливо це проявлялося під час атак на українські державні системи після 2014 року.

Атака на українські електромережі у грудні 2015 року показала новий рівень небезпеки кібероперацій. Зловмисники не просто проникли у систему, а отримали контроль над окремими елементами енергетичної інфраструктури. Після цього було дистанційно вимкнено підстанції, через що тисячі людей залишилися без електропостачання. Важливо те, що операція не обмежувалася одним вірусом або технічним збоєм. Перед втручанням проводилася тривала

підготовка - збір інформації про мережу, вивчення внутрішньої структури системи та доступів працівників. Це свідчило про цілеспрямований характер дій, а не про випадкову атаку хакерів.

Ще більш показовим став вірус NotPetya. Спочатку його поширення маскувалося під звичайне оновлення бухгалтерської програми. Після зараження система фактично втрачала працездатність. Проблема полягала у тому, що шкідливий код дуже швидко поширився за межі України. Під удар потрапили міжнародні перевізники, фармацевтичні компанії, виробничі підприємства та банки. У компанії Maersk через атаку було порушено роботу портової логістики у різних країнах світу. Частину серверів довелося відновлювати практично з нуля.

Цей випадок показав важливу особливість сучасних кібероперацій - відсутність чітких територіальних меж. Навіть якщо ціллю є одна держава, наслідки можуть одночасно зачепити десятки інших країн через глобальну взаємопов’язаність цифрових систем. Виникає проблема не лише індивідуальної відповідальності держави-організатора, а й міжнародної безпеки загалом.

Складність полягає ще й у тому, що кібератака не завжди має очевидний момент початку. Частина шкідливих програм роками перебуває всередині системи у пасивному режимі. Їх використовують для збору інформації або підготовки майбутнього втручання. Фактично держава може отримати прихований доступ до критичної інфраструктури іншої країни ще задовго до відкритого конфлікту.

Під час повномасштабної війни проти України кібероперації почали використовуватися паралельно з ракетними ударами та бойовими діями. Перед окремими атаками здійснювалися спроби втручання у системи зв’язку, державні сервіси та мережі супутникової комунікації. Атака на Viasat у лютому 2022 року вплинула не лише на український сегмент зв’язку, а й на роботу систем у країнах Європи.

Через це кіберпростір фактично перетворився на окрему сферу стратегічного контролю. Доступ до цифрової інфраструктури сьогодні має таке ж значення, як контроль над транспортними вузлами, енергетикою або військовими комунікаціями. Держави активно створюють кіберкомандування, спеціалізовані центри реагування та окремі підрозділи цифрової оборони. У багатьох країнах кібероперації вже офіційно включені до військового планування.

При цьому міжнародне право поки не встигає за швидкістю технологічних змін. Технічні можливості держав розвиваються значно швидше, ніж механізми юридичного реагування. Виникла ситуація, коли держави вже активно використовують кіберпростір як інструмент впливу, але міжнародна система відповідальності залишається фрагментарною та політично залежною.

Додаткові труднощі виникають через швидкоплинність цифрових доказів. Частина інформації може бути видалена автоматично, змінена або прихована ще до початку офіційного розслідування. У кібероперaціях значення мають технічні журнали, IP-адреси, шкідливий код, спосіб проникнення у систему та інші цифрові сліди. Однак навіть їх наявність не гарантує точного встановлення організатора атаки, оскільки одна й та сама інфраструктура може використовуватися різними суб’єктами.

Складною залишається і оцінка шкоди. Якщо наслідки ракетного удару можна зафіксувати одразу, то результати кібероперації іноді проявляються поступово. Втручання у державні бази даних або системи управління може залишатися непомітним протягом тривалого часу. Часто справжні масштаби шкоди виявляються лише після порушення роботи цілих секторів або втрати інформації. Зміна даних у реєстрах, втручання у фінансові системи чи поширення фальшивих повідомлень можуть створювати паніку серед населення навіть без фізичного пошкодження інфраструктури. Такі дії впливають на стабільність держави, але міжнародне право поки не містить чітких критеріїв оцінки подібних наслідків.

Практика останніх років показала, що кібероперації дедалі частіше стають частиною ширших військових або політичних кампаній. Їх використовують для підготовки до воєнних дій, дезорганізації систем управління, порушення зв’язку та ускладнення координації державних органів. У такому випадку цифрове втручання перестає бути ізольованим інцидентом і стає елементом загальної стратегії тиску на державу.

Через це міжнародна відповідальність у кіберпросторі вже не обмежується лише технічним аспектом. Вона напряму пов’язана з питаннями міжнародної безпеки, державного суверенітету та стабільності міжнародних відносин. Проблема правового реагування на кібероперації поступово переходить із вузькоспеціалізованої сфери у центральну площину сучасного міжнародного права.

Найбільш показовою у цьому контексті стала практика використання кібероперацій як елементу примусу без офіційного оголошення конфлікту. Держави отримали інструмент впливу, який дозволяє завдавати економічних та політичних втрат без формального перетину межі збройного нападу.

Наприклад, атаки на енергетичну інфраструктуру України у 2015 та 2016 роках не супроводжувалися офіційним визнанням участі конкретної держави, однак характер операцій свідчив про високий рівень підготовки, координації та доступу до спеціалізованих технічних ресурсів. Втручання було порушено електропостачання в регіонах, а сам інцидент став одним із перших випадків, коли кібератака безпосередньо вплинула на роботу енергосистеми держави. Це показало, що цифрові інструменти вже здатні створювати наслідки, які раніше асоціювалися виключно з фізичними диверсіями або військовими операціями.

Більш масштабними стали наслідки поширення шкідливого програмного забезпечення NotPetya у 2017 році. Первинно атака була спрямована на українські інформаційні системи через програмне забезпечення для бухгалтерського обліку, однак вірус швидко вийшов за межі початкової цілі. Було уражено міжнародні логістичні компанії, банківські структури,

промислові підприємства та державні установи у різних країнах світу. Загальні збитки оцінювалися у мільярди доларів [88]. Цей випадок продемонстрував, що навіть локальна кібероперація в умовах глобальної цифрової взаємозалежності може трансформуватися у міжнародну кризу.

Суттєво змінився і сам характер державного суверенітету. Якщо раніше суверенітет асоціювався переважно з контролем над територією, кордонами та населенням, то сьогодні до цього додається контроль над цифровою інфраструктурою та інформаційними потоками. Доступ до державних реєстрів, систем управління транспортом, банківських мереж або військових комунікацій фактично означає отримання можливості впливати на функціонування держави зсередини.

Проблема полягає у тому, що міжнародне право досі не виробило єдиного критерію, після якого кібероперація вважається достатньо небезпечною для застосування механізмів самооборони. Частина держав орієнтується на фізичні наслідки - руйнування об’єктів або людські жертви. Інші держави допускають можливість реагування і у випадках масштабної дестабілізації державних систем без фізичного знищення інфраструктури. Через це навіть серед союзників відсутня повна єдність щодо меж допустимої відповіді на кібератаки.

Додаткову небезпеку створює поєднання кібероперацій з інформаційними кампаніями. У сучасних конфліктах втручання у цифрові системи часто супроводжується поширенням дезінформації, маніпуляцією суспільною думкою та спробами підірвати довіру до органів влади. Така модель дій дозволяє впливати одночасно і на технічну інфраструктуру, і на психологічний стан суспільства.

Практика російсько-української війни підтвердила, що кібератаки можуть використовуватися синхронно з традиційними бойовими діями. У низці випадків втручання у системи зв’язку, державні сервіси або інформаційні мережі відбувалося безпосередньо перед ракетними ударами або під час активних бойових дій.

Фактично відбувається зміщення акценту - від епізодичних кібератак до системного використання цифрового середовища як інструменту міжнародного впливу. За таких умов проблема міжнародно-правової відповідальності вже не стосується лише інцидентів. Йдеться про формування нової моделі міжнародної безпеки, у межах якої кіберпростір став одним із ключових напрямів міждержавного протистояння.

Отже, сучасні кібероперації суттєво змінили підходи до розуміння міжнародно-правової відповідальності держав. Цифрове середовище створило нові форми втручання у внутрішні справи держав, які можуть завдавати значної шкоди без використання традиційної військової сили. Водночас анонімність, складність атрибуції та транснаціональний характер кіберпростору ускладнюють практичне застосування існуючих міжнародно-правових механізмів.

Попри відсутність спеціалізованого універсального договору щодо кібероперацій, міжнародне право вже містить базові принципи, які дозволяють оцінювати протиправні дії держав у цифровому середовищі. Йдеться насамперед про принципи суверенітету, невтручання, заборони застосування сили та норми міжнародного гуманітарного права. Однак сучасна практика свідчить, що наявних механізмів недостатньо для ефективного реагування на нові форми цифрових загроз.Начало формы

2.2. Форми та види міжнародно-правової відповідальності

Міжнародно-правова відповідальність за кібероперації реалізується через різні форми реагування держав та міжнародних організацій на порушення норм міжнародного права у цифровому середовищі. Особливість цієї сфери полягає у тому, що традиційні механізми відповідальності були сформовані для класичних міждержавних конфліктів і лише поступово адаптуються до кіберпростору.

У міжнародному праві відповідальність держав поділяється на матеріальну та нематеріальну. Матеріальна відповідальність передбачає обов’язок відшкодування шкоди, завданої міжнародно-протиправними діями. У сфері кібероперацій це питання є особливо складним через специфіку цифрової шкоди. На відміну від традиційних конфліктів, де збитки часто мають фізичний характер, кібератаки можуть призводити до втрати даних, блокування інформаційних систем, порушення роботи мереж або економічних втрат без прямого знищення об’єктів [16].

Одним із найбільш показових прикладів стала атака вірусу NotPetya у 2017 році. Унаслідок поширення шкідливого програмного забезпечення було порушено роботу банків, транспортних компаній, державних установ та промислових підприємств у різних країнах світу. Компанія Maersk тимчасово втратила контроль над частиною логістичних процесів, а відновлення цифрової інфраструктури потребувало значних фінансових витрат [88]. У таких випадках виникає питання про можливість компенсації збитків та механізм визначення відповідальної сторони.

Проблема полягає у тому, що міжнародне право не містить окремого універсального механізму компенсації шкоди, завданої кібероперaціями. Формально держава, яка порушила міжнародне зобов’язання, повинна забезпечити повне відшкодування наслідків протиправних дій [7]. Однак практична реалізація цього принципу залежить від можливості доведення причетності держави до конкретної атаки.

Нематеріальна відповідальність пов’язана із політичними та дипломатичними наслідками міжнародно-протиправних дій. У випадку кібероперацій ця форма відповідальності застосовується найчастіше. Держави використовують дипломатичні протести, міжнародне засудження, санкційні механізми, обмеження співпраці та інші форми політичного тиску. Подібна практика стала особливо поширеною після масштабних кібератак проти державних систем та критичної інфраструктури [11].

Європейський Союз поступово сформував окремий режим кіберсанкцій, спрямований на реагування на міжнародні кіберінциденти. Такі санкції можуть застосовуватися до фізичних осіб, організацій та структур, причетних до кібератак проти держав-членів ЄС або їхніх партнерів [78]. До санкційних заходів належать замороження активів, заборона фінансових операцій та обмеження на в'їзд. Важливо, що у цьому випадку відповідальність має не лише юридичний, а й превентивний характер, оскільки спрямована на стримування атак.

Подібний підхід застосовується і в межах НАТО. Альянс офіційно визнав кіберпростір окремим середовищем проведення операцій поряд із сушею, морем, повітрям та космосом [46]. НАТО не встановлює автоматичного механізму реагування на будь-який кіберінцидент. Рішення щодо застосування колективних механізмів захисту приймається залежно від масштабу наслідків атаки та рівня загрози для держав-членів [10].

У міжнародній практиці формується ще одна специфічна форма відповідальності - публічна атрибуція. Її суть полягає у відкритому покладенні відповідальності за кібератаку на конкретну державу без звернення до міжнародного суду.

Політичне значення публічної атрибуції полягає у формуванні міжнародного тиску та підриві можливості держави приховувати свою участь у кібероперaціях. Механізм не забезпечує повноцінної юридичної відповідальності, оскільки не передбачає обов'язкового судового рішення чи міжнародного примусу.

Відповідно до Проєкту статей про відповідальність держав, держава, яка постраждала від міжнародно-протиправного діяння, може застосовувати пропорційні заходи у відповідь з метою припинення порушення [7]. У кіберпросторі контрзаходи можуть включати санкції, обмеження доступу до технологій, припинення співпраці або навіть кібероперації у відповідь.

Питання допустимості «кібервідповіді» залишається одним із найбільш дискусійних у міжнародному праві. Частина держав вважає, що відповідь на

кібератаку може здійснюватися виключно у цифровому середовищі. Інші допускають можливість використання традиційних засобів самооборони у випадку, якщо наслідки кібератаки прирівнюються до збройного нападу [18].

Практика останніх років показує, що держави дедалі активніше використовують економічні та технологічні обмеження як форму відповідальності за кібероперації. Після масштабних кібератак окремі держави вводили експортні обмеження на постачання технологій, блокували доступ до цифрових платформ та обмежували співпрацю у сфері інформаційних технологій.

У сфері міжнародного гуманітарного права особливе значення має відповідальність за кібератаки на цивільну інфраструктуру. Женевські конвенції та Додаткові протоколи встановлюють заборону атак на цивільні об’єкти [2; 3]. У сучасних умовах це правило поширюється і на цифрові системи, від яких залежить життєзабезпечення населення. Йдеться про енергетичні мережі, медичні системи, транспортну інфраструктуру, системи водопостачання та зв’язку [14].

Кібератаки проти українських державних ресурсів, банківського сектору та енергетичної інфраструктури супроводжувалися інформаційними операціями та військовими діями. Такі дії створювали комплексний вплив на систему державного управління та цивільне населення.

Проблема міжнародно-правової відповідальності у цій сфері пов’язана також із відсутністю спеціалізованого міжнародного судового механізму щодо кібероперацій. Міжнародний Суд ООН розглядає міждержавні спори лише за згодою держав, а Міжнародний кримінальний суд зосереджений переважно на індивідуальній кримінальній відповідальності [5].

Через це міжнародна практика поступово зміщується у бік колективних механізмів реагування. Значну роль починають відігравати міжнародні організації, регіональні союзи та коаліції держав. Наприклад, у межах ООН держави працюють над формуванням принципів відповідальної поведінки у кіберпросторі [8]. ОБСЄ розвиває механізми довіри та обміну інформацією

щодо кіберінцидентів [12]. НАТО та ЄС посилюють координацію кіберзахисту та механізмів спільного реагування [10; 11].

Фактично міжнародно-правова відповідальність за кібероперації сьогодні формується одночасно у декількох площинах - юридичній, політичній, економічній та технологічній.

Показовим прикладом застосування політичної та санкційної форми відповідальності стала реакція держав Заходу на кібератаку SolarWinds, виявлену у 2020 році. Унаслідок компрометації програмного забезпечення компанії SolarWinds зловмисники отримали доступ до інформаційних систем федеральних органів США, дипломатичних структур та приватних компаній. Атака тривалий час залишалася непоміченою через складний механізм проникнення та використання легальних оновлень програмного забезпечення. Після проведення розслідування США офіційно поклали відповідальність на російські структури та запровадили санкції проти російських організацій і фізичних осіб, пов’язаних із кібероперaціями.

У випадку міжнародно-правова відповідальність реалізовувалася не через судову процедуру, а через політичні та економічні інструменти впливу. Водночас сам факт офіційного покладення відповідальності мав важливе міжнародне значення, оскільки демонстрував готовність держав публічно реагувати на кібероперації навіть за відсутності універсального механізму судового переслідування.

Прикладом стала атака на Colonial Pipeline у США у 2021 році. Унаслідок дій хакерського угруповання було тимчасово зупинено роботу найбільшого паливного трубопроводу на східному узбережжі США. Хоча формально атаку здійснила недержавна група DarkSide, американська сторона акцентувала увагу на тому, що діяльність подібних угруповань можлива через недостатнє реагування держави, на території якої вони функціонують.

Цей випадок став важливим для розвитку концепції «due diligence» - принципу належної обачності у кіберпросторі. Його суть полягає у тому, що держава повинна вживати заходів для недопущення використання власної

території або інфраструктури для здійснення кібератак проти інших держав [16]. Якщо держава не реагує на діяльність подібних груп, міжнародна спільнота може розглядати це як невиконання міжнародних зобов’язань.

Особливе місце у розвитку практики міжнародної відповідальності займають кібератаки проти України після 2022 року. Одразу після початку повномасштабного вторгнення було зафіксовано масові атаки на державні сайти, банківські системи, телекомунікаційні мережі та супутниковий зв’язок. Атака на супутникову мережу Viasat призвела до порушення роботи комунікацій не лише в Україні, а й у низці європейських держав. Пізніше Європейський Союз офіційно поклав відповідальність за цю операцію на Російську Федерацію [11].

Подібні атаки відбувалися паралельно із військовими діями. Це фактично підтвердило інтеграцію кібероперацій у сучасні воєнні кампанії. Втручання у цифрову інфраструктуру використовувалося для ускладнення зв’язку, порушення роботи державних сервісів та дестабілізації систем управління. У міжнародно-правовому контексті це створює підстави для застосування норм міжнародного гуманітарного права до кіберпростору [14].

Прикладом міжнародної координації у сфері реагування на кібероперації стала діяльність НАТО після масштабних атак на держави-члени Альянсу. У 2014 році кіберзахист був офіційно включений до системи колективної безпеки НАТО, а у кіберпростір визнано окремим операційним середовищем [46]. Це означає, що серйозна кібератака потенційно може розглядатися як загроза для всього Альянсу.

Практика показує, що держави поки уникають прямого військового реагування на кібероперації. Навіть у випадках масштабних атак основними інструментами залишаються санкції, дипломатичний тиск, публічна атрибуція та технологічні обмеження. Причина полягає у складності оцінки масштабів шкоди та ризику ескалації конфлікту. Наступний приклад це кібератака на парламент Німеччини у 2015 році. Унаслідок проникнення до інформаційних систем було викрадено значний обсяг даних депутатів та державних

службовців. Пізніше німецька влада офіційно пов’язала атаку з російськими хакерськими структурами. Реакцією стали санкції Європейського Союзу та міжнародне політичне засудження. У цьому випадку кібератака не спричинила фізичних руйнувань, однак була розцінена як загроза державному суверенітету та демократичним інститутам.

Ці приклади демонструють, що міжнародно-правова відповідальність у кіберпросторі поступово набуває практичного змісту навіть за відсутності єдиного міжнародного механізму примусу. Держави дедалі активніше використовують санкційні режими, міжнародну координацію та колективне реагування як спосіб стримування кібероперацій. Одночасно формується міжнародна практика, у межах якої кібератаки розглядаються не як суто технічні інциденти, а як дії, здатні порушувати міжнародну безпеку, суверенітет та стабільність міждержавних відносин.

Атака WannaCry привернула увагу не лише через масштаби поширення, а й через характер наслідків. У Великій Британії були тимчасово паралізовані окремі елементи системи NHS - національної служби охорони здоров’я. Лікарні втратили доступ до медичних баз даних, виникли перебої у роботі обладнання та записі пацієнтів. Частину операцій довелося переносити.

Раніше більшість підходів концентрувалася переважно на фізичних руйнуваннях або матеріальних збитках. Однак практика показала, що втручання у цифрові системи може мати не менш серйозні наслідки навіть без знищення об’єктів у класичному розумінні. Зупинка лікарні, порушення роботи енергосистеми або транспортної мережі впливають на базові умови функціонування держави та безпеку цивільного населення.

Наприклад, якщо внаслідок кібератаки держава зазнала масштабних економічних втрат, але не було людських жертв, міжнародне право не дає чіткої відповіді щодо допустимого рівня контрзаходів. Через це держави змушені формувати практику фактично у режимі реального часу, спираючись не лише на міжнародні договори, а й на політичні домовленості та власні безпекові інтереси. Цікаво, що у більшості сучасних кіберінцидентів реакція

держав має комбінований характер. Поряд із санкціями застосовуються дипломатичні обмеження, вислання представників дипломатичних місій, заборона співпраці у сфері технологій та публічне розкриття технічної інформації щодо проведеної атаки. Останній елемент став особливо важливим, оскільки технічна публікація методів атаки дозволяє іншим державам та компаніям підготуватися до аналогічних загроз.

Показовою у цьому сенсі стала діяльність CERT-UA під час повномасштабної війни. Українська сторона регулярно оприлюднювала інформацію про нові шкідливі програми, способи проникнення у системи та діяльність хакерських груп, пов’язаних із російськими структурами [59]. Фактично кіберзахист у сучасних умовах перестав бути виключно внутрішньою справою держави. Інформація про атаки швидко стає предметом міжнародного обміну між урядами, технічними центрами та приватними компаніями.

Значна частина міжнародного реагування формується не судами, а через координацію між державами та міжнародними організаціями. Наприклад, після низки атак на українську інфраструктуру Європейський Союз посилив співпрацю у сфері кібербезпеки, а НАТО активізувало обмін розвідувальною інформацією щодо кіберзагроз [10; 11].

При цьому міжнародно-правова відповідальність у кіберпросторі дедалі більше залежить від технічної експертизи. У багатьох випадках аналітичні звіти приватних компаній або спеціалізованих центрів стають основою для політичних рішень. Наприклад, Microsoft, Google Threat Analysis Group та інші структури регулярно публікують дані щодо діяльності державних хакерських груп, способів атак та цілей кібероперацій [26; 27]. Приватний сектор фактично став одним із учасників міжнародної системи реагування на кіберзагрози.

Помітно, що останніми роками держави почали сприймати кіберпростір не просто як технічне середовище, а як одну з ключових сфер національної безпеки. Особливо це стало помітно після атак на об’єкти критичної

інфраструктури. Наприклад, ситуація з Colonial Pipeline у США показала, наскільки сильно цифрові системи пов’язані з повсякденним функціонуванням держави. Після атаки виникли перебої з постачанням пального, а проблема дуже швидко вийшла за межі суто кібербезпеки. Йшлося вже не лише про злам системи, а про вплив на економіку, транспорт і суспільну стабільність.

У міжнародній практиці також поступово змінюється ставлення до атак на цивільну інфраструктуру. Якщо раніше головна увага приділялася військовим системам, то зараз очевидно, що найбільш вразливими часто є цивільні мережі. Енергетика, лікарні, банки, транспорт, державні реєстри - усе це залежить від цифрових технологій. Втручання у такі системи створює наслідки, які безпосередньо впливають на населення, навіть якщо фізичного руйнування об’єктів не відбулося.

Через це міжнародне гуманітарне право поступово почало адаптуватися до нових умов. У наукових дослідженнях та документах міжнародних організацій дедалі частіше підкреслюється, що цифрові системи, від яких залежить життєзабезпечення цивільного населення, повинні користуватися таким самим захистом, як і традиційні цивільні об’єкти [14]. На практиці це означає, що кібератаки на лікарні або енергетичні мережі можуть розглядатися як порушення міжнародного гуманітарного права.

Держава може роками заперечувати свою причетність до атаки, посилаючись на діяльність «незалежних» хакерських груп. Навіть за наявності технічних доказів міжнародна спільнота часто стикається з політичними обмеженнями.

Це добре видно на прикладі санкційної політики. Після великих кібератак держави все частіше застосовують економічні та технологічні обмеження. Йдеться не лише про блокування активів чи заборону в’їзду, а й про обмеження доступу до цифрових технологій, програмного забезпечення та електронних компонентів.

Показовим є і досвід України під час повномасштабної війни. Кібератаки стали постійною частиною конфлікту. Вони були спрямовані на державні сервіси, банки, телекомунікації, енергетичну інфраструктуру. Але одночасно стало помітно й інше - ефективна протидія таким атакам неможлива силами лише однієї держави. До захисту українських систем активно долучалися міжнародні компанії, іноземні урядові структури та спеціалізовані центри кібербезпеки [26; 59].

Фактично кіберпростір сформував нову модель міжнародної взаємодії, де питання безпеки вже не належать виключно до компетенції держави. Значну роль почали відігравати приватні технологічні компанії, які володіють інфраструктурою, програмними платформами та великими обсягами технічної інформації.

Усе це свідчить про те, що міжнародно-правова відповідальність у кіберпросторі поступово виходить за межі класичних підходів міжнародного права. Вона формується під впливом нових технологій, політичних факторів та змін у самій структурі міжнародної безпеки.

2.3. Індивідуальна кримінальна відповідальність

Начало формы

Проблема індивідуальної кримінальної відповідальності у сфері кібероперацій є значно складнішою, ніж у випадку традиційних міжнародних злочинів. Основна причина полягає у тому, що міжнародне кримінальне право формувалося переважно для реагування на воєнні злочини, злочини проти людяності, геноцид та злочин агресії, тобто діяння, які мають очевидний фізичний характер. Кіберпростір змінив сам механізм заподіяння шкоди. Сьогодні окремі дії у цифровому середовищі можуть створювати наслідки, співмірні з традиційними атаками, однак юридична кваліфікація таких дій досі залишається дискусійною [5; 16].

На відміну від міжнародно-правової відповідальності держав, індивідуальна кримінальна відповідальність стосується конкретних осіб - організаторів, виконавців, координаторів або осіб, які віддавали наказ щодо проведення кібероперації. У сучасних умовах такими суб'єктами можуть бути військові фахівці, працівники спецслужб, учасники хакерських груп або цивільні особи, які діяли в інтересах держави чи організованих структур.

Міжнародне право не містить окремого міжнародного договору, який би прямо встановлював кримінальну відповідальність за кібероперації. Проте це не означає, що подібні дії перебувають поза межами міжнародного кримінального права. Якщо наслідки кібероперації відповідають ознакам міжнародного злочину, відповідальність може наставати на підставі вже існуючих норм міжнародного права [5].

Найчастіше у цьому контексті згадується Римський статут Міжнародного кримінального суду. У документі прямо не використовується поняття «кібероперація», однак окремі кібератаки потенційно можуть підпадати під категорію воєнних злочинів або злочинів проти людяності. Йдеться насамперед про ситуації, коли цифрове втручання призводить до загибелі цивільного населення, руйнування критичної інфраструктури або створення гуманітарної катастрофи [5; 14].

Наприклад, якщо внаслідок кібератаки буде порушено роботу лікарень, систем життєзабезпечення або об'єктів енергетики, а це спричинить смерть людей чи масові страждання цивільного населення, подібні дії можуть розглядатися як порушення міжнародного гуманітарного права. У такому випадку відповідальність нестиме не лише держава, а і конкретні особи, які планували або здійснювали відповідну операцію.

Особливість кіберпростору полягає у тому, що одна людина або невелика група осіб може завдати масштабної шкоди без фізичної присутності на території іншої держави. Це суттєво відрізняє кібероперації від традиційних форм злочинної діяльності. Наприклад, шкідливе програмне забезпечення

може одночасно вражати системи у десятках країн, а виконавці атаки можуть перебувати за тисячі кілометрів від об’єкта втручання.

Показовим прикладом стала діяльність групи Sandworm, яку міжнародні експерти пов’язують із російськими військовими структурами. Цю групу пов’язували з атаками на українську енергосистему у 2015 році, поширенням вірусу NotPetya та іншими масштабними операціями [88]. У 2020 році Міністерство юстиції США офіційно висунуло обвинувачення шістьом громадянам Росії, яких вважали учасниками цієї групи. Їм інкримінували проведення атак проти України, Франції, Грузії та інших держав.

Цей випадок став важливим з кількох причин. По-перше, держави почали відкрито називати конкретних осіб, яких підозрюють у проведенні міжнародних кібероперацій. По-друге, кіберпростір перестав сприйматися як середовище повної анонімності. Навіть за складних механізмів приховування діяльності держави дедалі активніше використовують технічну розвідку, аналіз шкідливого коду та цифрові сліди для встановлення виконавців атак.

Притягнення таких осіб до відповідальності залишається складним. У більшості випадків підозрювані перебувають на території держав, які відмовляються від співпраці або не визнають обвинувачень. Через це кримінальне переслідування часто має символічний характер. Проте навіть публічне висунення обвинувачень створює міжнародні правові наслідки - обмеження пересування, санкції, міжнародний розшук та ускладнення міжнародної діяльності для таких осіб.

У сучасних війнах дедалі частіше використовуються не лише офіційні військові кіберпідрозділи, а і добровільні цифрові групи. Після початку повномасштабної війни проти України активно діяли різні хакерські об’єднання з обох сторін конфлікту. Частина з них атакувала державні ресурси, медіа, банківські системи та цифрову інфраструктуру.

У такій ситуації виникає проблема правового статусу подібних осіб. Якщо цивільна особа бере безпосередню участь у кібероперація під час

збройного конфлікту, вона може втратити захист, який міжнародне гуманітарне право надає цивільному населенню [2; 3].

Складною є і проблема доказування вини конкретної особи. У кіберпросторі виконавці використовують VPN-сервіси, мережі анонімізації, підставні сервери та інші способи приховування цифрових слідів. Крім того, окремі операції можуть проводитися колективно, коли різні учасники виконують лише частину дій і не мають повної інформації про всю операцію. Не кожна кібератака автоматично створює підстави для міжнародної кримінальної відповідальності. Більшість інцидентів кваліфікуються як кіберзлочини та розглядаються на рівні національного законодавства. У цьому контексті важливе значення має Конвенція про кіберзлочинність 2001 року, яка встановлює механізми міжнародної співпраці у сфері розслідування кіберзлочинів [6].

Однак коли кібероперація здійснюється у межах збройного конфлікту або призводить до тяжких наслідків для цивільного населення, виникає питання міжнародної кримінальної відповідальності. Тому сучасна міжнародна практика поступово рухається до розширення застосування норм міжнародного кримінального права на цифрове середовище.

На практиці проблема безкарності у кіберпросторі значною мірою пов’язана із транснаціональним характером цифрових операцій. Людина, яка організовує атаку, може перебувати в одній державі, використовувати сервери в іншій, а наслідки її дій виникатимуть одночасно у кількох країнах. Через це класичний механізм кримінальної юрисдикції, побудований переважно на територіальному принципі, у сфері кібероперацій працює значно менш ефективно.

Наприклад, під час розслідування міжнародних кібератак правоохоронні органи часто стикаються з необхідністю отримання цифрових доказів із різних юрисдикцій. Для цього потрібна міжнародна правова допомога, однак у багатьох випадках процес займає надто багато часу. Частина інформації може бути втрачена ще до отримання офіційного дозволу на доступ до серверів або

електронних даних. У сфері кіберзлочинності швидкість реагування має принципове значення.

Конвенція про кіберзлочинність 2001 року стала одним із перших міжнародних документів, який передбачив механізми співпраці держав у сфері розслідування кіберзлочинів [6]. Документ встановив процедури обміну інформацією, збереження електронних доказів та взаємодії між правоохоронними органами. Однак Конвенція створювалася переважно для боротьби з класичними кіберзлочинами - незаконним доступом до систем, шахрайством, втручанням у дані або поширенням шкідливих програм. Сучасні кібероперації у межах міжнародних конфліктів значно виходять за ці межі.

Особливо це стало помітно після початку активного використання кібератак у міждержавному протистоянні. Наприклад, атаки на українську енергосистему або державні ресурси мали не лише кримінальний, а й стратегічний характер. Їхньою метою було не особисте збагачення чи отримання інформації, а дестабілізація функціонування держави.

Міжнародне кримінальне право поки не виробило окремої категорії «міжнародного кіберзлочину». Через це правова кваліфікація залежить від наслідків конкретної операції. Якщо кібератака спричинила загибель людей, порушення роботи лікарень, енергетичних систем або інших критично важливих об’єктів, вона потенційно може розглядатися як воєнний злочин [14]. Якщо ж наслідки обмежуються викраденням інформації або тимчасовим порушенням роботи систем, питання міжнародної кримінальної відповідальності залишається відкритим. Частина сучасного шкідливого програмного забезпечення здатна самостійно поширюватися мережею, змінювати власний код та адаптуватися до систем захисту. У таких випадках виникає складне питання - якою мірою особа повинна відповідати за наслідки, які вийшли за межі початкового плану операції.

Прикладом стала ситуація з вірусом NotPetya. Первинно атака була спрямована проти українських систем, однак через механізм самостійного поширення шкідливе програмне забезпечення швидко вийшло з-під контролю

та уразило міжнародні компанії у різних країнах світу [88]. Це створило нову проблему для міжнародного права - відповідальність за непрогнозовані наслідки цифрових операцій.

У традиційному міжнародному гуманітарному праві існує принцип розрізнення між військовими та цивільними об’єктами [2; 3]. У кіберпросторі реалізувати цей принцип значно складніше, оскільки одна й та сама цифрова інфраструктура часто використовується одночасно і цивільними, і військовими структурами. Наприклад, телекомунікаційні мережі або супутниковий зв’язок можуть забезпечувати як цивільні сервіси, так і військову координацію. Через це навіть атака на об’єкт із військовим значенням може спричинити масштабні наслідки для цивільного населення.

Питання індивідуальної кримінальної відповідальності у сфері кібероперацій поступово набуває не лише юридичного, а й етичного значення. Особи, які планують або здійснюють кібератаки, дедалі частіше впливають на безпеку мільйонів людей без прямого фізичного контакту із жертвами. У сучасних умовах один цифровий інструмент може порушити роботу лікарень, транспортних систем, енергетики чи державного управління одразу у кількох країнах.

Додаткову складність створює те, що у кіберпросторі межа між державним виконавцем і цивільною особою часто є розмитою. У традиційних конфліктах приналежність до збройних сил зазвичай можна встановити через форму, структуру підпорядкування або офіційний статус. У цифровому середовищі одна й та сама особа може одночасно працювати у приватній ІТ-компанії, брати участь у діяльності хакерських груп і виконувати завдання в інтересах держави. Це ускладнює визначення її правового статусу та меж відповідальності.

Під час сучасних конфліктів дедалі частіше використовуються моделі так званої «неформальної кібермобілізації». Держава прямо не включає хакерські групи до структури збройних сил, однак фактично заохочує їхню діяльність або використовує результати їхніх атак у власних інтересах. Така

практика стала помітною після початку повномасштабної війни проти України, коли у кіберпросторі активізувалася велика кількість різних угруповань. Частина з них атакувала державні ресурси, медіаплатформи, банківські системи та цифрові сервіси.

Більшість осіб, причетних до кібероперацій, переслідуються на рівні національного законодавства. Держави самостійно визначають склади кіберзлочинів, процедури розслідування та покарання. Водночас у випадках міжнародних конфліктів або атак проти критичної інфраструктури питання вже виходить за межі внутрішньої юрисдикції.

Міжнародна співпраця відіграє важливу роль між правоохоронними органами. Однак практика показує, що така взаємодія часто залежить від політичних відносин між державами. Якщо країна відмовляється видавати підозрюваних або не визнає факт проведення кібероперації, механізм міжнародного переслідування суттєво ускладнюється. Тому у багатьох справах щодо міжнародних кібератак обвинувальні акти існують формально, але реального судового процесу не відбувається.

Навіть символічне кримінальне переслідування має значення для міжнародної практики. Воно поступово формує принцип невідворотності відповідальності за дії у кіберпросторі. Публічне встановлення осіб, причетних до кібератак, міжнародний розшук, санкції та обмеження пересування створюють додатковий механізм стримування, навіть якщо фактичне затримання таких осіб залишається малоймовірним.

Сучасна практика також демонструє поступове розширення міжнародної співпраці у сфері цифрових доказів. Для розслідування кібероперацій держави використовують технічну експертизу, аналіз шкідливого коду, мережеву аналітику та дані приватних технологічних компаній. Цифрові сліди сьогодні стали основним джерелом доказової бази у справах про міжнародні кібероперації.

Цифрові докази мають специфічний характер. Вони можуть швидко змінюватися, копіюватися або знищуватися. Технічна інформація часто

потребує складної експертної оцінки, яка недоступна без спеціалізованих знань. Через це у справах щодо кібероперацій дедалі більшу роль відіграють експерти з кібербезпеки, аналітичні центри та приватні компанії, які фактично беруть участь у формуванні доказової бази.

Фактично міжнародне кримінальне право сьогодні змушене адаптуватися до ситуації, у якій джерелом загрози може бути не лише держава або військове формування, а і невелика група технічно підготовлених осіб, здатних дистанційно впливати на критичну інфраструктуру інших держав.

У практиці російсько-української війни це проявилося особливо чітко. Частина кібератак була спрямована на телекомунікаційні мережі, супутниковий зв'язок та державні цифрові сервіси. Формально такі системи могли використовуватися для координації державних структур, однак їх порушення одночасно впливало і на цивільне населення - доступ до зв'язку, банківських операцій, електронних документів та інформаційних ресурсів. Оцінка наслідків кібероперацій у сучасних конфліктах вже не може обмежуватися лише технічним аналізом пошкоджених систем. Значення має реальний вплив на безпеку людей та функціонування суспільства [14; 72].

Показовою стала атака на супутникову мережу Viasat у лютому 2022 року. Порушення роботи супутникових терміналів вплинуло не лише на українські системи зв'язку, а і на роботу мереж у країнах Європи. Унаслідок цього виникли перебої у функціонуванні комунікаційної інфраструктури, зокрема у сфері дистанційного управління обладнанням [11]. Цей випадок показав, що одна цифрова операція здатна створювати наслідки одночасно у кількох державах, а отже питання кримінальної відповідальності перестає бути суто внутрішньою справою конкретної країни.

У сучасних умовах високий рівень технічної підготовки часто зосереджений у приватному секторі, а не у державних структурах. Через це держави можуть залучати до кібероперацій програмістів, системних адміністраторів, фахівців із мережевої безпеки або аналітиків без формального включення таких осіб до складу збройних сил.

Міжнародне гуманітарне право у цьому питанні виходить із принципу безпосередньої участі у воєнних діях [2; 3]. Однак стосовно кіберпростору цей підхід залишається недостатньо визначеним. Наприклад, якщо особа створює програмний код для атаки на енергосистему або забезпечує технічну підтримку кібероперації, її діяльність може мати прямий вплив на хід конфлікту. Водночас у міжнародному праві відсутній чіткий механізм визначення моменту, коли цифрова діяльність цивільної особи перетворюється на безпосередню участь у воєнних діях. На це звертають увагу автори Tallinn Manual 2.0 [16].

У багатьох конфліктах подібні об’єднання формально діють самостійно, однак фактично координують свою діяльність із політичними або військовими інтересами держави. Частина таких груп займається DDoS-атаками, зламом державних ресурсів, поширенням шкідливого програмного забезпечення або втручанням у інформаційні системи. При цьому держава може офіційно не визнавати зв’язок із подібними структурами, що значно ускладнює як міжнародно-правову, так і індивідуальну кримінальну відповідальність.

На практиці це створює ситуацію правової невизначеності. З одного боку, діяльність таких груп може мати наслідки, співмірні з військовими операціями. З іншого боку, міжнародне право поки не виробило універсального механізму кваліфікації подібних дій. Більшість держав намагається вирішувати питання через національні механізми кримінального переслідування або санкційні процедури [6; 7].

Кібероперації часто супроводжуються психологічним та інформаційним впливом. У сучасних конфліктах втручання у цифрові системи поєднується з дезінформацією, поширенням панічних повідомлень та спробами підірвати довіру до державних інституцій. Наприклад, під час атак на державні ресурси України одночасно поширювалися повідомлення про нібито втрату державних баз даних або повне знищення цифрової інфраструктури. Часто реальні технічні наслідки були значно меншими, ніж інформаційний ефект від атаки.

Практика показує, що міжнародна система реагування поки значною мірою відстає від темпів розвитку технологій. Кібероперація може бути проведена за декілька годин, тоді як міжнародне розслідування триває роками. Часто на момент офіційного встановлення виконавців цифрова інфраструктура вже змінена, сервери ліквідовані, а самі учасники операції продовжують діяльність під іншими технічними ідентифікаторами.

Серйозною проблемою для міжнародного кримінального переслідування є також питання екстериторіальності кібероперацій. У більшості випадків цифрова атака не прив'язана до конкретної території у класичному розумінні. Командний сервер може знаходитися в одній країні, виконавець - в іншій, а уражені системи - одразу у декількох державах. Через це виникає конфлікт юрисдикцій та проблема визначення держави, яка має пріоритетне право на кримінальне переслідування.

У традиційному кримінальному праві основним критерієм зазвичай є місце вчинення злочину. У кіберпросторі цей підхід працює лише частково. Наприклад, якщо атака здійснювалася через інфраструктуру кількох держав, а наслідки виникли на території інших країн, встановлення «місця злочину» фактично втрачає однозначність.

Особливо це стосується атак на виборчі системи, державні бази даних або урядові інформаційні мережі. У таких випадках навіть відсутність матеріальних збитків не зменшує рівень загрози, оскільки основний вплив спрямований на політичну стабільність та функціонування державних інституцій. Показовим був випадок із кібератакою на Бундестаг у Німеччині у 2015 році. Унаслідок проникнення до парламентських мереж було викрадено значний обсяг інформації, включаючи електронне листування депутатів та службові документи. Німецька сторона публічно заявила про причетність російських хакерських структур, а згодом Європейський Союз застосував санкції щодо осіб, яких пов'язували з організацією атаки [11]. У цій ситуації основна загроза полягала не у фізичному пошкодженні систем, а у втручанні у діяльність державного органу та отриманні доступу до політично чутливої

інформації. На відміну від традиційних речових доказів, електронна інформація є нестабільною та легко змінюється. Дані можуть автоматично видалятися, перезаписуватися або шифруватися.

Складність полягає і в тому, що цифровий доказ сам по собі не завжди дозволяє встановити конкретного виконавця. Наприклад, використання однакового шкідливого коду різними групами не означає автоматичної причетності однієї держави. Частина інструментів потрапляє у відкритий доступ після витоку даних або використовується повторно іншими угрупованнями. Через це міжнародна атрибуція кібероперацій майже завжди базується на сукупності факторів - технічному аналізі, характері цілі, способах проведення атаки та політичному контексті.

У практиці останніх років держави дедалі частіше поєднують кримінальне переслідування із санкційними механізмами. Наприклад, щодо осіб, підозрюваних у проведенні міжнародних кібератак, можуть одночасно застосовуватися фінансові обмеження, заборона на в’їзд, блокування активів та міжнародний розшук.

За відсутності реального арешту подібні заходи поступово формують міжнародну практику персональної відповідальності у цифровому середовищі. Якщо на початку розвитку кіберпростору атаки сприймалися переважно як анонімна діяльність без конкретного суб’єкта, то зараз міжнародна спільнота дедалі активніше переходить до моделі персоніфікації відповідальності.

Конкретним прикладом персоніфікації відповідальності стала справа проти співробітників російського ГРУ, яким Міністерство юстиції США у 2020 році висунуло обвинувачення у проведенні низки міжнародних кібероперацій. Серед епізодів фігурували атаки на українську енергетичну систему, поширення NotPetya, втручання у французькі виборчі процеси та атаки під час зимових Олімпійських ігор у Пхьончхані [88]. Особливість цієї справи полягала у тому, що вперше на міжнародному рівні були публічно

названі конкретні особи, військові підрозділи та механізми проведення кібероперацій.

Фактично йшлося вже не про абстрактну «хакерську активність», а про системну діяльність державних структур. У матеріалах розслідування детально описувалися способи проникнення у мережі, використані шкідливі програми, маршрути передачі даних та цифрова інфраструктура.

Показовою є і справа щодо втручання у виборчу систему США у 2016 році. Американська сторона офіційно висунула обвинувачення окремим громадянам Росії, яких пов'язували з кібератаками на сервери Демократичної партії та операціями з поширення викраденої інформації. У цьому випадку міжнародна проблема полягала не лише у незаконному доступі до даних. Основна загроза розглядалася як спроба впливу на демократичні процеси та внутрішньополітичну стабільність держави.

Після таких інцидентів питання кібероперацій почало розглядатися у контексті захисту демократичних інституцій. Втручання у вибори, державні інформаційні системи або парламентські мережі дедалі частіше кваліфікується як загроза суверенітету держави, навіть якщо фізичного пошкодження інфраструктури не відбулося [17].

На увагу заслуговує проблема використання програм-вимагачів (ransomware). Формально значна частина таких атак має кримінально-економічний характер і спрямована на отримання викупу за відновлення доступу до системи. Однак останніми роками подібні інструменти почали використовуватися і в контексті міждержавного протистояння. Наприклад, окремі угруповання здійснювали атаки на державні установи, лікарні, транспортні компанії та енергетичні об'єкти.

Атака на Colonial Pipeline у 2021 році стала одним із найбільш показових випадків. Через втручання у систему управління найбільшого паливного трубопроводу США компанія була змушена тимчасово зупинити роботу. Це спричинило перебої з постачанням пального у декількох штатах та панічні закупівлі серед населення. Хоча операцію офіційно пов'язували з групою

DarkSide, ситуація показала, наскільки серйозними можуть бути наслідки діяльності навіть недержавних кіберугруповань.

Після цього інциденту американська влада посилила політику щодо переслідування операторів ransomware-груп, а проблема кіберзлочинності почала розглядатися не лише як питання правоохоронної діяльності, а і як фактор національної безпеки.

У сучасних умовах дедалі більше значення має також питання командної відповідальності у кіберпросторі. У традиційному міжнародному гуманітарному праві командир може нести відповідальність за злочини підлеглих, якщо він знав або повинен був знати про їх вчинення та не вжив необхідних заходів [54]. У цифровому середовищі реалізація цього принципу значно складніша через багаторівневу структуру кібероперацій та використання неформальних виконавців.

Наприклад, якщо атака здійснюється через афілійовану хакерську групу, формально не включену до структури державних органів, виникає питання щодо меж відповідальності посадових осіб, які координували або санкціонували таку діяльність.

Український досвід також демонструє, що кібероперації дедалі частіше використовуються як елемент комплексного тиску під час війни. Атаки на державні реєстри, банківську систему, медіаресурси та енергетичну інфраструктуру відбувалися паралельно із бойовими діями.

Отже, розвиток цифрових технологій суттєво змінив підходи до індивідуальної кримінальної відповідальності у міжнародному праві. Кібероперації створили нову категорію загроз, у межах якої окремі особи або організовані групи здатні впливати на функціонування держав, критичної інфраструктури та безпеку цивільного населення без безпосереднього фізичного контакту з об’єктом атаки.

Сучасна практика демонструє, що міжнародна спільнота поступово переходить від сприйняття кібероперацій як суто технічних інцидентів до розуміння їх як дій, здатних створювати наслідки міжнародно-правового

масштабу. Висунення обвинувачень конкретним особам, застосування санкцій, міжнародний розшук та використання цифрових доказів свідчать про формування механізмів персональної відповідальності у кіберпросторі [5; 16].

Складність атрибуції, транснаціональний характер цифрових атак, використання неформальних виконавців та швидка зміна технологій суттєво ускладнюють ефективне кримінальне переслідування. Крім того, міжнародне право поки не містить спеціалізованого універсального режиму відповідальності за кібероперації, що створює значну правову невизначеність.

Попри це, практика останніх років підтверджує, що кіберпростір уже став повноцінною сферою міжнародного протистояння, а питання індивідуальної кримінальної відповідальності у цифровому середовищі набуває дедалі більшого значення для міжнародної безпеки, захисту цивільного населення та забезпечення стабільності міжнародного правопорядку.

Отже, розвиток цифрових технологій та активне використання кібероперацій у сучасних конфліктах зумовлюють необхідність подальшого вдосконалення міжнародно-правових механізмів притягнення фізичних осіб до відповідальності за міжнародно-протиправні дії у кіберпросторі. Сучасна практика демонструє, що кібероперації можуть створювати наслідки, співмірні з результатами традиційних форм збройного насильства, а тому питання ефективного міжнародно-правового реагування на такі дії поступово стає одним із ключових напрямів розвитку міжнародного гуманітарного права та системи міжнародної безпеки загалом.

Начало формы

РОЗДІЛ 3. РОЗВИТОК МІЖНАРОДНО-ПРАВОВИХ МЕХАНІЗМІВ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРОПЕРАЦІЇ: ПРОБЛЕМИ ТА ПРАКТИКА СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТІВ

3.1. Сучасні міжнародні ініціативи та практика регулювання кібероперацій в умовах збройних конфліктів

Особливе значення мав звіт Групи урядових експертів ООН 2021 року. У документі держави фактично підтвердили, що діяльність у кіберпросторі не перебуває поза межами міжнародного права, а тому принципи суверенітету, невтручання у внутрішні справи держав, мирного врегулювання спорів та заборони застосування сили повинні застосовуватися і до цифрового середовища [8].

Основна суперечність стосується питання контролю над цифровим середовищем. США, держави Європейського Союзу та більшість західних країн підтримують концепцію відкритого глобального Інтернету, де ключове значення мають свобода інформації та багатостороннє управління цифровою мережею. Натомість Китай, Росія та частина інших держав просувають концепцію «цифрового суверенітету», відповідно до якої держава повинна мати максимально широкий контроль над власним інформаційним простором [13; 48].

Через ці відмінності міжнародне співтовариство досі не змогло виробити універсальний міжнародний договір, який би комплексно регулював кібероперації. Більшість існуючих документів мають рекомендаційний або політичний характер.

Однією з найбільш активних структур у цій сфері є НАТО. Після кібератак на Естонію у 2007 році проблема цифрової безпеки стала одним із пріоритетів Альянсу [10]. Тоді масовані атаки на державні сайти, банки та телекомунікаційні мережі фактично паралізували частину цифрової інфраструктури країни. Хоча фізичного руйнування об'єктів не відбулося, ситуація продемонструвала, наскільки залежною стала держава від стабільності інформаційних систем.

Після цього НАТО суттєво посилило кіберполітику та створило нові механізми координації у сфері цифрової безпеки. У 2008 році було посилено роль NATO Cooperative Cyber Defence Centre of Excellence у Таллінні, який поступово перетворився на один із головних міжнародних центрів дослідження правових аспектів кібероперацій [37; 76]. На базі цього центру був підготовлений Tallinn Manual 2.0 - документ, який став одним із найавторитетніших джерел тлумачення міжнародного права у сфері кіберпростору [16].

Хоча Tallinn Manual не є міжнародним договором і не має юридично обов'язкової сили, його значення для міжнародної практики є надзвичайно великим. У документі вперше системно проаналізовано застосування міжнародного гуманітарного права, права міжнародної безпеки та норм відповідальності держав до кібероперацій. Експерти дійшли висновку, що окремі кібератаки можуть кваліфікуватися як застосування сили або навіть як збройний напад, якщо наслідки таких дій співмірні з наслідками традиційного військового втручання [16; 18].

Важливим є і те, що Tallinn Manual приділяє увагу питанням захисту цивільного населення під час кіберконфліктів. У документі наголошується, що принципи розрізнення, пропорційності та необхідності, які існують у

міжнародному гуманітарному праві, повинні застосовуватися і до цифрових операцій [2; 3; 16]. Це означає, що атаки на цивільну інфраструктуру, лікарні або системи життєзабезпечення можуть розглядатися як порушення міжнародного гуманітарного права навіть тоді, коли шкода завдається через цифрове втручання.

Практичне значення таких підходів стало особливо помітним у сучасних конфліктах. Наприклад, у ході російсько-української війни кібератаки неодноразово здійснювалися проти енергетичної інфраструктури, державних сервісів, телекомунікаційних систем та банківського сектору. У багатьох випадках цифрові операції використовувалися одночасно із ракетними ударами або інформаційними кампаніями.

Європейський Союз також поступово формує власу систему реагування на кіберзагрози. У ЄС кібербезпека дедалі більше розглядається як елемент стратегічної автономії та захисту критичної інфраструктури [11; 78]. Після масштабних атак останніх років у межах Євросоюзу були створені механізми координації між державами-членами, системи обміну інформацією про кіберінциденти та механізми санкцій за проведення міжнародних кібератак.

Особливе значення мало створення так званого EU Cyber Diplomacy Toolbox - механізму, який дозволяє Європейському Союзу застосовувати дипломатичні та санкційні заходи у відповідь на шкідливу кібердіяльність. Фактично це стало першим випадком, коли регіональна організація створила спеціальний механізм політичного реагування на кібероперації.

Показовим є те, що сучасна міжнародна практика дедалі частіше використовує санкції як один із головних способів реагування на кібератаки. Наприклад, після атак на Бундестаг, втручання у вибори або кібератак на українську інфраструктуру ЄС, США та інші держави застосовували обмеження щодо осіб і структур, яких вважали причетними до відповідних операцій [11]. Таким чином формується новий механізм міжнародної відповідальності, у якому поряд із класичними юридичними процедурами активно використовуються політичні та економічні інструменти впливу.

ОБСЄ у питаннях кібербезпеки зробила акцент не стільки на покаранні, скільки на недопущенні конфліктів через цифрові інциденти. Організація почала просувати механізми швидкої комунікації між державами, обмін інформацією про кіберзагрози та створення постійних контактних пунктів для реагування на інциденти [12].

Практичне значення, оскільки у багатьох випадках держави не можуть оперативно встановити, чи була атака дією окремої хакерської групи, елементом роботи спецслужб або частиною ширшої воєнної операції. Особливо це стосується ситуацій, коли кібератака відбувається одночасно з політичною кризою або збройним конфліктом. У таких умовах ризик помилкової ескалації значно зростає.

Наприклад, після атак на Естонію у 2007 році у міжнародному середовищі фактично не існувало готового механізму реагування на подібні інциденти. Кібератаки тоді паралізували роботу банків, урядових сайтів та медіаресурсів, але водночас не було чіткого розуміння, чи можна розглядати це як загрозу міжнародній безпеці у класичному сенсі [16]. Цей випадок став одним із переломних моментів для міжнародної дискусії щодо правового статусу кібероперацій.

Поступово держави почали усвідомлювати, що цифрове середовище вже не є допоміжним елементом сучасного конфлікту. Воно стало окремим напрямом протистояння, де можна впливати на державу без прямого застосування військової сили. Причому ефект від таких дій іноді виявляється не менш серйозним, ніж від традиційних атак. Порушення роботи енергосистеми, транспортної інфраструктури або державних сервісів здатне створити масштабну дестабілізацію навіть без фізичного руйнування об’єктів.

Через це у міжнародному праві почала змінюватися сама оцінка наслідків кібероперацій. Якщо раніше головним критерієм вважалася фізична шкода, то зараз дедалі більше уваги приділяється впливу на функціонування держави та безпеку цивільного населення. Наприклад, атака на систему

лікарень або державні цифрові сервіси може безпосередньо впливати на життя людей навіть без використання зброї у традиційному розумінні [14].

Це особливо добре видно на прикладі російсько-української війни. Починаючи з 2014 року Україна стала фактично полігоном для нових форм кібероперацій. Атаки були спрямовані проти енергетики, банківської системи, телекомунікацій, державних реєстрів та інформаційних ресурсів. Одним із найбільш показових випадків стали атаки на українську енергосистему у 2015 та 2016 роках, коли через втручання у системи управління частина споживачів залишилася без електропостачання [59].

Ці інциденти мали велике значення для міжнародної практики, оскільки вперше було продемонстровано можливість реального фізичного впливу через цифрове втручання. До цього кібератаки переважно асоціювалися з викраденням даних або блокуванням інформаційних систем. Український випадок показав, що наслідком цифрової операції може бути безпосереднє порушення роботи критичної інфраструктури.

Первинно шкідливе програмне забезпечення поширювалося через українське бухгалтерське програмне забезпечення, однак дуже швидко вийшло за межі України та вразило міжнародні компанії у різних країнах світу [88].

Після NotPetya міжнародна спільнота почала значно серйозніше сприймати проблему кібероперацій у контексті міжнародної безпеки. Кілька держав офіційно поклали відповідальність за атаку на Росію, а питання міжнародної атрибуції кібератак вийшло на новий рівень [11]. Важливо, що реакція полягала не лише у політичних заявах. Держави почали активніше застосовувати санкції, обмеження у сфері технологій та механізми колективного реагування.

Якщо раніше вони переважно виконували функцію майданчиків для обговорення, то зараз дедалі активніше беруть участь у формуванні практичних механізмів координації кіберзахисту. Помітно, що сучасне міжнародне регулювання кібероперацій дедалі більше зміщується у бік

практичної координації, а не лише декларативних заяв. Причина полягає у тому, що цифрові атаки розвиваються значно швидше, ніж міжнародно-правові механізми. Держави фактично були змушені реагувати на нові загрози ще до появи чітких універсальних правил. Значна частина сучасної системи кібербезпеки формується через політичні домовленості, міждержавну співпрацю та технічну взаємодію.

Особливо це стало помітно після початку повномасштабної війни проти України. Уперше в історії масштабного міжнародного конфлікту кібероперації використовувалися практично безперервно паралельно із бойовими діями. Атаки здійснювалися проти державних органів, телекомунікаційної інфраструктури, банківської системи, медіаресурсів та енергетики. При цьому цифрові операції часто поєднувалися з інформаційними кампаніями та ракетними ударами.

Наприклад, перед окремими атаками на енергетичну інфраструктуру фіксувалися спроби проникнення у системи управління або порушення роботи інформаційних сервісів. Така синхронізація показала, що кіберпростір більше не розглядається як допоміжний інструмент. Він став окремою складовою сучасної воєнної стратегії.

На цьому фоні суттєво посилилася роль приватних технологічних компаній. У попередніх міжнародних конфліктах ключовими суб’єктами безпеки були держави та військові союзи. У цифровому середовищі ситуація інша, оскільки значна частина інфраструктури перебуває у приватному секторі. Хмарні сервіси, телекомунікаційні мережі, програмні платформи та системи кіберзахисту належать міжнародним компаніям, які фактично стали учасниками процесу забезпечення безпеки.

Під час війни в Україні це проявилося дуже чітко. Microsoft, Google, Amazon, Starlink та інші технологічні структури брали участь у захисті цифрової інфраструктури, перенесенні державних даних у хмарні системи, виявленні шкідливого програмного забезпечення та підтримці комунікацій

[26; 27]. Фактично приватний сектор став елементом міжнародної системи протидії кіберзагрозам.

Великі технологічні компанії сьогодні володіють обсягом інформації та технічними можливостями, які іноді перевищують ресурси держав. Вони часто першими фіксують кібератаки, аналізують шкідливий код та встановлюють механізми діяльності хакерських груп. Через це міжнародне регулювання кіберпростору вже неможливо розглядати виключно через міждержавні механізми.

Держави дедалі сильніше залежать від приватної цифрової інфраструктури, а отже питання безпеки частково виходить за межі прямого державного контролю. Наприклад, рішення технологічної компанії щодо доступу до сервісів, зберігання даних або роботи мережевої інфраструктури може впливати на стійкість держави під час конфлікту.

Після атак на енергосистеми, лікарні та транспортні мережі міжнародна спільнота почала приділяти значно більше уваги об’єктам, від яких залежить функціонування цивільного населення. У документах ООН та міжнародних організацій дедалі частіше наголошується на необхідності утримуватися від кібератак проти медичних установ, систем водопостачання, енергетики та інших об’єктів життєзабезпечення [8; 14].

Проблема полягає у тому, що ці принципи поки не мають достатньо жорсткого механізму забезпечення. Міжнародне право у сфері кібероперацій значною мірою продовжує спиратися на добровільне дотримання норм державами.

Проте поступово формується практика, за якої кібератаки на критичні цивільні об’єкти починають сприйматися як серйозне порушення міжнародної безпеки. Особливо помітно після атак на лікарні та енергосистеми, коли цифрове втручання створювало прямі ризики для життя населення. У таких випадках міжнародна дискусія вже виходить за межі технічної кібербезпеки та переходить у площину гуманітарного права й захисту цивільних осіб під час конфліктів.

Практика показала, що ефективність реагування на кібератаки напряму залежить від швидкості передачі технічної інформації між державами, міжнародними організаціями та приватними структурами. У цифровому середовищі навіть кілька годин затримки можуть призвести до масштабного поширення шкідливого програмного забезпечення або втрати контролю над системами.

Останніми роками активно розвиваються міжнародні механізми координації CERT-команд та центрів реагування на кіберінциденти. Такі структури займаються технічним аналізом атак, виявленням нових вразливостей та обміном інформацією щодо способів захисту [59]. Фактично йдеться про створення міжнародної мережі оперативної кібербезпеки, яка працює паралельно із класичними дипломатичними механізмами.

Показово, що у випадку великих міжнародних атак інформація про шкідливе програмне забезпечення часто поширюється значно швидше через технічні канали співпраці, ніж через офіційні міждержавні процедури. Тобто це підтверджує, що сучасне регулювання кіберпростору має не лише юридичний, а й виражений технічний характер. Без технологічної координації навіть найрозвиненіші міжнародно-правові механізми залишаються малоефективними.

Помітну роль у формуванні сучасної практики відіграють також аналітичні та дослідницькі центри. Такі структури, як NATO CCDCOE, RAND Corporation, Atlantic Council, CSIS та Carnegie Endowment, фактично стали учасниками міжнародної дискусії щодо правил поведінки у кіберпросторі [61; 64; 65; 66]. Їхні дослідження активно використовуються під час розробки державних стратегій кібербезпеки та міжнародних підходів до регулювання цифрових конфліктів.

Держави часто не встигають адаптувати законодавство до нових технологій, тому значну частину аналітичної роботи виконують наукові та експертні центри., технічні стандарти та доктринальні підходи.У багатьох випадках кібератака використовується не лише для порушення роботи систем,

а і для створення психологічного ефекту, паніки або недовіри до державних інституцій.

Через це міжнародні організації дедалі частіше розглядають кібербезпеку у ширшому контексті інформаційної стійкості держави. Йдеться вже не лише про захист серверів або мережевої інфраструктури, а і про здатність держави підтримувати стабільність управління, комунікацій та довіру суспільства під час цифрових криз.

На рівні Європейського Союзу це проявилося у розвитку концепції цифрової стійкості. ЄС почав активно інвестувати у захист критичної інфраструктури, розвиток спільних стандартів кіберзахисту та посилення безпеки цифрових сервісів [11]. Особлива увага приділяється енергетиці, транспортним системам, фінансовому сектору та медичній сфері, оскільки ці напрямки вважаються найбільш вразливими до масштабних кібератак.

Сучасна практика також демонструє поступове зближення військової та цивільної сфер у питаннях кібербезпеки. Більшість цифрової інфраструктури, яка використовується державами, одночасно обслуговує і цивільні потреби. Через це атака на телекомунікаційну мережу або супутниковий зв’язок майже завжди має подвійний ефект - військовий та цивільний. Така особливість робить кібероперації надзвичайно складними для міжнародно-правового регулювання.

У міжнародному гуманітарному праві існує принцип розмежування між цивільними та військовими об’єктами [2; 3]. Однак у цифровому середовищі провести таке розмежування значно важче. Наприклад, одна й та сама хмарна платформа може використовуватися державними структурами, лікарнями, банками та військовими підрозділами одночасно. Через це сучасні конфлікти демонструють, що навіть точкова кібератака здатна створити масштабні непрямі наслідки для цивільного населення.

Отже, сучасні міжнародні ініціативи у сфері регулювання кібероперацій демонструють поступовий перехід від суто політичних декларацій до формування практичних механізмів міжнародної взаємодії у цифровому

середовищі. Міжнародні організації, регіональні безпекові структури та окремі держави дедалі активніше розглядають кіберпростір як одну з ключових сфер міжнародної безпеки, що безпосередньо впливає на стабільність міжнародних відносин та функціонування державного суверенітету.

Практика сучасних збройних конфліктів підтвердила, що кібероперації стали повноцінним елементом воєнного протистояння. Атаки на енергетичну інфраструктуру, державні інформаційні системи, телекомунікаційні мережі та цифрові сервіси продемонстрували здатність кіберпростору впливати не лише на технічну сферу, а і на економіку, державне управління та безпеку цивільного населення. Особливо це проявилося під час російсько-української війни, де цифрові атаки використовувалися паралельно із військовими та інформаційними операціями.

Проведене дослідження показало, що сучасна система міжнародно-правового регулювання кібероперацій залишається недостатньо цілісною. Відсутність універсального міжнародного договору, складність атрибуції кібератак, різні підходи держав до питання цифрового суверенітету та швидкий розвиток технологій суттєво ускладнюють формування єдиного механізму міжнародної відповідальності у кіберпросторі.

Попри це, міжнародна практика свідчить про поступове формування нових підходів до регулювання цифрових конфліктів. Діяльність ООН, НАТО, Європейського Союзу, ОБСЄ та спеціалізованих центрів кібербезпеки сприяє виробленню спільних принципів поведінки держав у цифровому середовищі, розвитку механізмів міжнародної координації та посиленню захисту критичної інфраструктури.

3.2. Проблеми та напрями вдосконалення норм міжнародного гуманітарного права щодо кібероперацій

Начало формы

Конец формы

Начало формы

Конец формы

Начало формы

Стрімкий розвиток цифрових технологій показав, що існуючі норми міжнародного гуманітарного права не були розраховані на сучасний рівень кіберзагроз. Більшість міжнародно-правових механізмів формувалися у період, коли основною формою збройного впливу залишалося фізичне застосування сили. Натомість сучасні кібероперації здатні створювати масштабні наслідки без традиційного військового втручання.

Відсутність чіткої термінології безпосередньо впливає на питання міжнародної відповідальності та застосування міжнародного гуманітарного права. Наприклад, одні держави розглядають масштабне втручання у цифрову інфраструктуру як форму застосування сили, інші - як інформаційний або технічний інцидент, який не досягає рівня збройного нападу. Через це міжнародна реакція на подібні дії часто залежить не від єдиного правового стандарту, а від політичної позиції конкретної держави.

У міжнародному праві відповідальність держави можлива лише за умови доведення її причетності до міжнародно-протиправного діяння [7]. У кіберпросторі це завдання значно ускладнюється через використання підставної інфраструктури, VPN-сервісів, серверів третіх країн та афілійованих хакерських груп. Часто навіть за наявності технічних доказів держави офіційно заперечують свою причетність до атак.

Практика останніх років показує, що міжнародна атрибуція дедалі частіше базується не лише на технічному аналізі, а і на політичних та розвідувальних даних. Однак така модель створює ризик суб’єктивності та політизації процесу встановлення відповідальності.

Показово, що після початку повномасштабної війни проти України проблема кібербезпеки фактично стала складовою міжнародної системи оборони. У дослідженнях НАТО Cooperative Cyber Defence Centre of

Excellence наголошується, що сучасні конфлікти дедалі більше поєднують військові, інформаційні та цифрові інструменти впливу [76; 77]. Це означає, що міжнародне гуманітарне право вже не може розглядати кіберпростір як допоміжний елемент воєнних дій.

Український досвід підтвердив, що кібератаки здатні використовуватися для дестабілізації державного управління та створення додаткового тиску на цивільне населення. У матеріалах CERT-UA неодноразово фіксувалися спроби втручання у державні системи, поширення шкідливого програмного забезпечення та атаки на об’єкти критичної інфраструктури [59]. Частина таких операцій була спрямована не лише на технічне пошкодження систем, а і на створення паніки, порушення роботи державних сервісів та підрив довіри до цифрової інфраструктури держави.

У документах Європейського Союзу та ENISA наголошується, що енергетика, транспорт, фінансовий сектор та системи охорони здоров’я залишаються найбільш вразливими до масштабних кібератак [78; 79].

Проблема полягає у тому, що міжнародне гуманітарне право формувалося у період, коли критична інфраструктура не мала настільки високого рівня цифрової інтеграції. Сьогодні ж одна кібератака може одночасно порушити роботу електромереж, систем зв’язку, банківських сервісів та державного управління.

У звітах Microsoft Digital Defense Report також зазначається, що сучасні державні кібероперації дедалі частіше спрямовані не на короткочасний ефект, а на тривале проникнення у системи та підготовку до можливого масштабного втручання у майбутньому [80]. Це означає, що частина цифрових загроз може залишатися прихованою роками, а сам факт втручання виявляється лише після початку активної фази конфлікту.

Серед основних напрямів удосконалення міжнародного гуманітарного права сьогодні називають розробку чіткіших критеріїв атрибуції кібератак, визначення меж застосування сили у цифровому середовищі, посилення захисту цивільної цифрової інфраструктури та створення міжнародних

механізмів швидкого реагування на масштабні кіберінциденти. Без адаптації міжнародного права до сучасних технологічних реалій ефективне регулювання кібероперацій у майбутньому залишатиметься суттєво обмеженим.

На відміну від традиційних видів озброєння, цифрові інструменти практично неможливо повністю контролювати або обмежувати через класичні механізми міжнародного права. Шкідливе програмне забезпечення може копіюватися, модифікуватися та швидко поширюватися між різними суб'єктами. Після витоку або використання окремі елементи кіберзброї нерідко потрапляють у відкритий доступ та починають застосовуватися вже іншими групами.

Сталося це після витоку інструментів Агентства національної безпеки США, коли частина шкідливих програм була використана у міжнародних кібератаках. Найбільш показовим прикладом став вірус WannaCry, який у 2017 році вразив сотні тисяч комп'ютерів у різних країнах світу. Постраждали лікарні, транспортні системи, підприємства та державні установи. У Великій Британії атака серйозно вплинула на роботу National Health Service, через що частину медичних операцій довелося скасувати [79; 80].

Цей випадок показав, наскільки небезпечним є поширення цифрових інструментів ураження без міжнародного контролю. Якщо традиційна зброя потребує виробництва, логістики та фізичного переміщення, то шкідливий код може бути переданий миттєво та використаний будь-де у світі. Глобальний характер Інтернету, міжнародна хмарна інфраструктура та діяльність транснаціональних технологічних компаній створюють ситуацію, коли частина критично важливих цифрових ресурсів перебуває поза прямим державним контролем. У дослідженнях RAND Corporation та Atlantic Council наголошується, що майбутні конфлікти будуть ще більш залежними від цифрових технологій, автоматизованих систем та штучного інтелекту [85; 86]. Це означає, що проблема правового регулювання кібероперацій у найближчі роки лише посилюватиметься. Уже зараз міжнародне право стикається із

ситуацією, коли технології розвиваються швидше, ніж механізми їх юридичного врегулювання.

Фактично сучасне міжнародне гуманітарне право поступово переходить до нового етапу розвитку, де питання безпеки вже неможливо відокремити від цифрового середовища.Начало формы

Конец формы

У традиційних міжнародних конфліктах для фіксації порушень можуть використовуватися місії спостерігачів, міжнародні слідчі групи або спеціальні комісії. У кіберпросторі така модель працює значно складніше. Для проведення повноцінного розслідування необхідний доступ до серверів, журналів подій, мережевої інфраструктури та технічних даних, які часто перебувають у різних юрисдикціях або належать приватним компаніям.

На практиці це призводить до ситуації, коли міжнародна оцінка кібератаки значною мірою залежить від інформації, яку надає сама постраждала держава або великі технологічні компанії. Через це питання довіри до цифрових доказів стає одним із ключових у міжнародних кіберконфліктах. Особливо гостро ця проблема проявляється у політично чутливих ситуаціях, коли держави взаємно звинувачують одна одну у проведенні кібератак.

Держави дедалі активніше посилюють контроль над цифровим середовищем, пояснюючи це необхідністю захисту від кібератак та інформаційних загроз. Однак на практиці це нерідко супроводжується розширенням систем цифрового спостереження, контролю за комунікаціями та обмеженням доступу до інформації.

Особливо складним це питання стає під час воєнних конфліктів, коли держави отримують додаткові повноваження у сфері інформаційної безпеки та контролю над цифровими ресурсами. Соціальні мережі, месенджери, супутниковий зв’язок та хмарні сервіси під час сучасних конфліктів часто виконують одночасно цивільні й військові функції. Наприклад, цифрові

платформи можуть використовуватися для координації гуманітарної допомоги, але одночасно - для передачі військової інформації або навігації.

Через це виникає складне питання щодо правового статусу таких об’єктів. З одного боку, вони залишаються цивільною інфраструктурою. З іншого - їх використання у військових цілях може робити їх потенційною ціллю для кібероперацій. У сучасних умовах міжнародне гуманітарне право поступово стикається із необхідністю переосмислення самого поняття воєнного середовища. Якщо раніше основними просторами конфлікту були суша, море та повітря, то зараз повноцінним елементом бойових дій став цифровий простір. Причому його особливість полягає у тому, що межа між тилом і зоною бойових дій фактично стирається. Кібератака може одночасно впливати на державні установи, цивільне населення, міжнародні компанії та об’єкти інфраструктури у різних країнах.

Отже, сучасний розвиток цифрових технологій створив для міжнародного гуманітарного права низку принципово нових викликів, які неможливо повноцінно врегулювати виключно за допомогою традиційних правових механізмів. Кібероперації суттєво змінили характер сучасних конфліктів, оскільки дозволяють впливати на державу, критичну інфраструктуру та цивільне населення без прямого фізичного застосування сили.

Проведене дослідження показало, що основними проблемами сучасного міжнародно-правового регулювання кібероперацій залишаються складність атрибуції кібератак, відсутність універсального визначення меж застосування сили у цифровому середовищі, труднощі розмежування цивільних і військових об’єктів, а також недостатня ефективність механізмів міжнародної відповідальності. Додаткові труднощі створюють використання недержавних хакерських груп, глобальний характер цифрової інфраструктури та стрімкий розвиток нових технологій, зокрема систем штучного інтелекту.

Практика сучасних конфліктів, насамперед російсько-української війни, підтвердила, що кіберпростір став повноцінною сферою міжнародного

протистояння. Кібератаки на енергетичну систему, телекомунікації, державні сервіси та інші об’єкти критичної інфраструктури продемонстрували здатність цифрових операцій створювати масштабні наслідки для функціонування держави та безпеки цивільного населення навіть без фізичного руйнування об’єктів.

Начало формы

Конец формы

3.3. Практика кібероперацій у російсько-українській війні та проблеми притягнення до міжнародно-правової відповідальності

Російсько-українська війна стала одним із перших масштабних міжнародних конфліктів, у якому кібероперації системно використовувалися паралельно з традиційними бойовими діями. Якщо раніше кібератаки переважно розглядалися як допоміжний інструмент інформаційного або технічного впливу, то після 2014 року цифровий простір фактично перетворився на окремий напрям воєнного протистояння. Україна стала державою, на території якої були апробовані різні моделі кібервтручання - від атак на державні інформаційні системи до операцій проти критичної інфраструктури та телекомунікаційних мереж.

Перші масштабні кібератаки проти України були зафіксовані ще у 2014 році після початку окупації Криму та бойових дій на сході України. Основними цілями стали державні органи, медіаресурси, телекомунікаційні системи та інформаційна інфраструктура. Уже тоді стало очевидно, що цифрові операції використовуються не лише для збору інформації, а і для дестабілізації внутрішньої ситуації в державі.

Особливу увагу міжнародної спільноти привернули атаки на українську енергосистему у 2015 та 2016 роках. Втручання у системи управління частина споживачів залишилася без електропостачання [59]. Це був один із перших випадків у світовій практиці, коли кібератака безпосередньо вплинула на

функціонування енергетичної інфраструктури держави. Важливо, що наслідки мали не лише технічний характер. Порушення електропостачання впливало на роботу транспорту, зв'язку, банківських систем та інших сфер життєзабезпечення населення.

Після цих інцидентів міжнародні організації та дослідницькі центри почали серйозніше оцінювати ризики кібератак проти критичної інфраструктури [72; 77]. Український випадок показав, що цифрове втручання може створювати реальні наслідки для цивільного населення без застосування традиційної зброї. Це стало одним із аргументів на користь необхідності адаптації міжнародного гуманітарного права до сучасних кіберзагроз.

Наступним етапом ескалації стала атака вірусу NotPetya у 2017 році. Формально шкідливе програмне забезпечення поширювалося через оновлення українського бухгалтерського сервісу M.E.Doc, однак дуже швидко атака вийшла за межі України та набула глобального масштабу. Постраждали міжнародні транспортні компанії, банки, промислові підприємства та логістичні мережі у різних державах світу [88]. Загальні збитки оцінювалися у мільярди доларів.

Особливість NotPetya полягала у тому, що вірус фактично не був орієнтований на отримання фінансового прибутку. Попри зовнішню схожість із програмами-вимагачами, основною метою було саме знищення та блокування інформаційних систем. Це суттєво відрізняло атаку від класичної кіберзлочинності та свідчило про її дестабілізаційний характер. У міжнародному середовищі NotPetya почали розглядати як один із прикладів використання кібероперацій для завдання масштабної економічної шкоди державі та міжнародним компаніям.

Після цієї атаки низка держав офіційно поклала відповідальність на Росію. США, Велика Британія, Канада, Австралія та держави Європейського Союзу публічно заявили про причетність російських військових структур до організації операції [11]. Це стало одним із найбільш показових прикладів міжнародної політичної атрибуції кібератаки. Водночас навіть за наявності

публічних заяв механізм реального міжнародно-правового притягнення до відповідальності залишився обмеженим.

Проблема полягала у тому, що міжнародне право досі не містить спеціального механізму відповідальності саме за проведення кібероперацій такого масштабу. Після початку повномасштабного вторгнення у 2022 році інтенсивність кібератак проти України суттєво зросла. При цьому цифрові операції почали використовуватися вже не епізодично, а фактично як постійний компонент воєнної кампанії. Основними цілями стали державні інформаційні ресурси, енергетика, супутниковий зв'язок, телекомунікації та фінансовий сектор.

Однією з перших масштабних атак стала операція проти супутникової мережі Viasat у лютому 2022 року. Унаслідок втручання було виведено з ладу тисячі супутникових терміналів, які використовувалися не лише в Україні, а і в інших європейських країнах [11]. Особливість цього випадку полягала у тому, що наслідки кібератаки вийшли далеко за межі території держави, проти якої вона була спрямована. Це ще раз підтвердило глобальний характер сучасних кібероперацій та складність їх локалізації.

Паралельно із технічними атаками активно використовувалися інформаційно-психологічні операції. Злами державних сайтів часто супроводжувалися поширенням дезінформації, фейкових повідомлень або спробами створити паніку серед населення. Такий підхід демонструє, що у сучасних конфліктах цифровий простір використовується не лише для технічного впливу, а і для психологічного тиску на суспільство.

На відміну від програм-вимагачів, такі шкідливі програми не передбачають можливості відновлення даних після сплати викупу. Їхнє завдання полягає саме у руйнуванні цифрової інфраструктури. Під час війни проти України подібні програми неодноразово використовувалися проти державних установ та критичних об'єктів [26; 80]. У міжнародному праві такі дії створюють серйозну проблему кваліфікації. Формально цифрове втручання може не супроводжуватися фізичним руйнуванням об'єкта, однак фактичні

наслідки для державного управління та цивільного населення можуть бути співмірними із результатами традиційних атак. Саме це зараз є одним із головних предметів міжнародної дискусії щодо адаптації міжнародного гуманітарного права до реалій кіберпростору.

Суттєвою особливістю російсько-української війни стало і те, що Україна фактично стала центром міжнародної координації у сфері кіберзахисту. Після 2022 року допомога Україні почала включати не лише постачання озброєння чи фінансову підтримку, а і співпрацю у сфері цифрової безпеки. До захисту української інфраструктури активно долучилися міжнародні технологічні компанії, спеціалізовані центри кібербезпеки та урядові структури партнерських держав.

Наприклад, Microsoft повідомляла про системне виявлення шкідливих програм, які використовувалися проти українських державних органів та критичної інфраструктури [80]. Компанія брала участь у перенесенні державних даних до хмарних середовищ, що дозволило зменшити ризики втрати інформації внаслідок фізичних атак або цифрового знищення серверів. Подібна практика фактично створила новий формат міжнародної взаємодії, у якому приватні технологічні структури стали важливими учасниками забезпечення національної та міжнародної безпеки.

Основна складність полягає у процедурі доведення причетності держави до конкретної операції. У більшості випадків кібератаки проводяться через багаторівневу інфраструктуру, підставні сервери або афілійовані хакерські групи. Це дозволяє державам уникати прямого визнання участі у цифрових операціях навіть тоді, коли атака відповідає їхнім військовим або політичним інтересам.

Проблемною є і оцінка шкоди від цифрових атак. У традиційному міжнародному праві наслідки зазвичай визначаються через фізичне руйнування або людські втрати. У кіберпросторі значна частина шкоди має функціональний характер - порушення роботи систем, втрату доступу до інформації, дестабілізацію управління або економічні збитки.

Російсько-українська війна також показала, що кібероперації здатні впливати не лише на державу, а і на міжнародну безпеку загалом. Атаки на супутникові системи, міжнародні логістичні мережі або глобальні програмні платформи створюють ризики для багатьох держав одночасно. Це означає, що сучасний кіберконфлікт уже не може розглядатися виключно як внутрішня проблема окремої держави.

Отже, практика кібероперацій у російсько-українській війні підтвердила, що цифровий простір став повноцінною сферою сучасного міжнародного протистояння. Кібератаки використовуються як інструмент дестабілізації державного управління, впливу на критичну інфраструктуру, психологічного тиску на населення та супроводу бойових дій. Водночас міжнародна практика показала суттєву обмеженість існуючих механізмів міжнародно-правової відповідальності у сфері кібероперацій. Складність атрибуції, відсутність спеціалізованих міжнародних механізмів реагування та швидкий розвиток цифрових технологій створюють ситуацію, у якій міжнародне право поки не встигає адаптуватися до реалій сучасних кіберконфліктів.

ВИСНОВКИ

1. Проведене дослідження дозволило встановити, що кібероперації у сучасних міжнародних відносинах перетворилися на один із ключових інструментів реалізації державної політики у сфері безпеки та оборони. Стрімкий розвиток цифрових технологій та формування глобального кіберпростору призвели до трансформації традиційних підходів до розуміння міжнародних конфліктів. На відміну від класичних форм застосування сили, кібероперації характеризуються нематеріальним характером, високою швидкістю здійснення, відсутністю чітких територіальних меж та можливістю прихованого впливу на державу. Це свідчить про формування нової моделі міжнародного протистояння, у якій інформаційні технології відіграють не менш важливу роль, ніж традиційні військові засоби.

2. У ході дослідження встановлено, що міжнародне право наразі не містить універсального визначення поняття «кібероперація». Така ситуація пояснюється історичним розвитком міжнародно-правових норм, більшість яких була сформована ще до виникнення кіберпростору як окремого середовища міжнародної взаємодії. У зв’язку з цим ключову роль у формуванні сучасних підходів до розуміння кібероперацій відіграють міжнародно-правова доктрина, аналітичні дослідження та експертні

документи. Особливе значення у цьому контексті має Tallinn Manual 2.0, який систематизує підходи до визначення кібероперацій, застосування міжнародного гуманітарного права та встановлення міжнародно-правової відповідальності у цифровому середовищі.

3. Доведено, що кібероперації можуть бути кваліфіковані як форма застосування сили або збройного нападу у випадку, коли їх наслідки є співмірними з наслідками традиційних військових дій. Визначальне значення у цьому випадку мають не технічні способи реалізації кібератаки, а характер, масштаб та інтенсивність її наслідків. Кібероперації, спрямовані на виведення з ладу енергетичних систем, транспортної інфраструктури, банківського сектору, систем зв'язку або медичних установ, здатні створювати загрозу життю та здоров'ю населення, що дозволяє розглядати їх як сучасну форму застосування сили у міжнародних відносинах.

4. Встановлено, що кібероперації суттєво змінюють уявлення про просторові межі міжнародного конфлікту. На відміну від традиційних військових дій, які пов'язані з конкретною територією, кібероперації можуть здійснюватися дистанційно та одночасно охоплювати об'єкти, розташовані у різних державах. Це ускладнює застосування принципу територіального суверенітету та створює проблеми у сфері визначення юрисдикції держав. У сучасних умовах територіальний фактор поступово втрачає свою визначальну роль, оскільки кіберпростір не має чітких фізичних меж.

5. У роботі доведено, що застосування норм міжнародного гуманітарного права до кібероперацій супроводжується значними труднощами. Принципи розрізнення, пропорційності, гуманності та військової необхідності були сформовані для традиційних форм ведення війни та потребують адаптації до особливостей цифрового середовища. Високий рівень взаємозалежності сучасних інформаційних систем ускладнює прогнозування наслідків кібероперацій, а також визначення меж допустимого впливу на цивільну інфраструктуру.

6. Встановлено, що однією з основних проблем міжнародно-правової відповідальності у кіберпросторі є проблема атрибуції. Використання технологій маскування, бот-мереж, проміжних серверів, викрадених облікових записів та інфраструктури третіх держав значно ускладнює процес встановлення суб’єкта, відповідального за здійснення кібератаки. Відсутність належних доказів створює труднощі для покладення міжнародно-правової відповідальності на державу та суттєво обмежує можливості міжнародного реагування на кіберзагрози.

7. Дослідження показало, що кібероперації характеризуються високим рівнем мультиакторності. На відміну від традиційних збройних конфліктів, у кіберпросторі активну роль відіграють не лише держави, але й недержавні суб’єкти – хакерські угруповання, приватні компанії, організовані групи та окремі особи. Така особливість ускладнює застосування міжнародного гуманітарного права, яке історично орієнтоване насамперед на регулювання діяльності держав. У зв’язку з цим виникає необхідність удосконалення міжнародно-правових механізмів відповідальності з урахуванням сучасного характеру кіберзагроз.

8. Визначено, що правовий статус даних та цифрової інформації у системі міжнародного гуманітарного права залишається недостатньо визначеним. Втручання у функціонування інформаційних систем, знищення або модифікація даних можуть мати наслідки, співмірні із фізичним руйнуванням об’єктів. Водночас чинні міжнародно-правові норми не містять чітких критеріїв оцінки подібної шкоди. Це створює прогалини у правовому регулюванні та ускладнює кваліфікацію відповідних дій.

9. У ході дослідження встановлено, що кібероперації дедалі частіше використовуються як елемент гібридної війни. Їх застосування поєднується з інформаційними кампаніями, економічним тиском, політичним впливом та іншими формами дестабілізації держави. Це свідчить про комплексний характер сучасних конфліктів, у межах яких кіберпростір використовується як окремий інструмент стратегічного впливу.

10. Доведено, що розвиток цифрових технологій значно випереджає темпи формування міжнародно-правових норм. Більшість існуючих міжнародних договорів була прийнята до виникнення сучасного кіберпростору, що зумовлює необхідність адаптації міжнародного гуманітарного права до нових технологічних реалій. Відсутність спеціалізованих універсальних міжнародних актів у сфері кібероперацій створює ситуацію нормативної невизначеності та ризик неоднакового тлумачення права різними державами.

11. У роботі встановлено, що важливу роль у формуванні сучасної системи міжнародної кібербезпеки відіграє міжнародне співробітництво. Ефективна протидія кіберзагрозам потребує координації дій держав, міжнародних організацій, наукових установ та приватного сектору. Особливого значення набуває обмін інформацією про кіберінциденти, створення спільних механізмів реагування та вироблення єдиних міжнародних стандартів у сфері кібербезпеки.

12. Визначено, що сучасні кібероперації становлять серйозну загрозу для критичної інформаційної інфраструктури держав. Енергетичні системи, транспортні мережі, банківський сектор, системи зв’язку та медичні установи значною мірою залежать від цифрових технологій, а тому є вразливими до кібератак. Порушення їх функціонування може спричинити масштабні економічні, соціальні та гуманітарні наслідки, співмірні із наслідками традиційних військових дій.

13. Практика російсько-української війни підтвердила, що кібероперації стали невід’ємним елементом сучасних збройних конфліктів. Кібератаки використовуються для порушення функціонування державних органів, критичної інфраструктури, інформаційних систем та комунікаційних мереж. Водночас такі дії поєднуються з інформаційними операціями та психологічним впливом на населення, що свідчить про комплексний характер сучасної гібридної війни.

14. Для України питання забезпечення кібербезпеки має стратегічне значення в умовах триваючої збройної агресії Російської Федерації. Підвищення рівня захисту критичної інформаційної інфраструктури, розвиток системи кіберзахисту, удосконалення механізмів реагування на кіберінциденти та посилення міжнародного співробітництва повинні стати одними з ключових напрямів державної політики у сфері національної безпеки.

15. Проведене дослідження дає підстави стверджувати, що кібероперації у сучасних умовах набули ознак самостійного інструменту міжнародного протистояння, який поєднує технічні, політичні, інформаційні та правові складові. Їх використання дозволяє державам досягати стратегічних цілей без прямого застосування традиційної збройної сили, що суттєво змінює підходи до розуміння безпеки, суверенітету та характеру міжнародних конфліктів. У зв’язку з цим виникає необхідність подальшого вдосконалення міжнародно-правового регулювання діяльності у кіберпросторі.

16. Встановлено, що застосування міжнародного гуманітарного права у кіберпросторі ускладнюється відсутністю чітких міжнародних процедур документування та розслідування кіберінцидентів. Для встановлення міжнародно-правової відповідальності необхідне належне підтвердження факту втручання, однак цифрові сліди можуть бути змінені, приховані або повністю знищені. Це суттєво знижує ефективність міжнародних механізмів реагування та створює передумови для уникнення відповідальності за міжнародно-протиправні дії у кіберпросторі.

17. Дослідження показало, що важливу роль у сучасних кібероперація відіграють автоматизовані системи та технології штучного інтелекту. Їх використання дозволяє здійснювати кібератаки з високою швидкістю, адаптувати способи впливу до систем захисту та реалізовувати складні багаторівневі операції без безпосереднього втручання людини. Це створює нові виклики для міжнародного права, оскільки традиційні підходи

до встановлення вини та відповідальності не враховують специфіку автономних цифрових систем.

18. Встановлено, що сучасний кіберпростір функціонує на основі складної взаємодії держав, міжнародних організацій, приватного сектору та технічних спільнот. Значна частина критичної цифрової інфраструктури перебуває у власності приватних компаній, які забезпечують функціонування інформаційних систем, телекомунікаційних мереж та цифрових сервісів. У зв’язку з цим ефективне забезпечення кібербезпеки неможливе без налагодження постійної взаємодії між державними органами та приватним сектором.

19. Доведено, що кібероперації безпосередньо впливають на систему міжнародної безпеки та трансформують підходи до стримування у міжнародних відносинах. На відміну від традиційних військових засобів, кібероперації характеризуються високим рівнем анонімності та прихованості, що ускладнює демонстрацію сили та застосування класичних механізмів стримування. У сучасних умовах держави дедалі частіше використовують кіберпростір як середовище постійного стратегічного тиску, що змінює характер міжнародного протистояння.

20. У ході дослідження встановлено, що кібероперації можуть становити загрозу не лише для міжнародної безпеки, але й для прав і свобод людини. Втручання у роботу інформаційних систем здатне призводити до обмеження доступу до інформації, порушення права на приватність, блокування цифрових сервісів та поширення дезінформації. Це свідчить про необхідність комплексного застосування норм міжнародного гуманітарного права та міжнародного права прав людини у процесі регулювання діяльності у кіберпросторі.

21. Визначено, що сучасні кібероперації характеризуються високим рівнем складності та багатофазністю. Вони можуть включати проникнення до інформаційних систем, закріплення у мережі, приховане збирання інформації, модифікацію даних та подальше порушення функціонування об’єктів

інфраструктури. Така специфіка свідчить про поступову інституціоналізацію кібероперацій як окремого елементу сучасних військових та безпекових стратегій держав.

22. Доведено, що відсутність єдиних міжнародних стандартів у сфері кваліфікації кібероперацій створює ризик неоднакового тлумачення міжнародного права державами. Різні підходи до визначення поняття кібератаки, застосування сили та збройного нападу ускладнюють формування єдиного міжнародного механізму реагування на кіберзагрози. Це негативно впливає на ефективність міжнародного співробітництва та стримує розвиток універсальної системи міжнародно-правової відповідальності.

23. Установлено, що ефективний захист критичної інформаційної інфраструктури потребує комплексного підходу, який включає не лише технічні засоби кіберзахисту, але й удосконалення нормативно-правового забезпечення, розвиток міжнародної співпраці та підготовку висококваліфікованих фахівців. У сучасних умовах кібербезпека повинна розглядатися як невід'ємна складова національної та міжнародної безпеки.

24. Практика російсько-української війни засвідчила, що кібероперації використовуються як складова гібридної агресії та поєднуються з інформаційними кампаніями, психологічним впливом і традиційними військовими діями. Кібератаки проти державних органів, енергетичних систем, телекомунікаційної інфраструктури та інформаційних ресурсів України підтвердили необхідність посилення міжнародних механізмів захисту держав у цифровому середовищі та вдосконалення системи міжнародно-правового реагування на подібні загрози.

25. Підсумовуючи результати проведеного дослідження, слід зазначити, що подальший розвиток міжнародного гуманітарного права у сфері регулювання кібероперацій повинен бути спрямований на формування універсальних міжнародно-правових норм, які б визначали критерії кваліфікації кібероперацій, механізми атрибуції, особливості притягнення до міжнародно-правової відповідальності та гарантії захисту цивільної

інфраструктури у кіберпросторі. Лише комплексне вдосконалення міжнародно-правового регулювання здатне забезпечити ефективне реагування на сучасні кіберзагрози та підвищити рівень міжнародної безпеки в умовах цифровізації міжнародних відносин.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Статут Організації Об'єднаних Націй від 26.06.1945 [Електронний ресурс]. – Режим доступу: https://www.un.org/en/about-us/un-charter (дата звернення: 04.05.2026).

2. Женевські конвенції від 12.08.1949 [Електронний ресурс]. – Режим доступу: https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf (дата звернення: 04.05.2026).

3. Додатковий протокол I до Женевських конвенцій від 08.06.1977 [Електронний ресурс]. – Режим доступу: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977 (дата звернення: 04.05.2026).

4. Додатковий протокол II до Женевських конвенцій від 08.06.1977 [Електронний ресурс]. – Режим доступу: https://ihl-databases.icrc.org/en/ihl-treaties/apii-1977 (дата звернення: 04.05.2026).

5. Римський статут Міжнародного кримінального суду від 17.07.1998 [Електронний ресурс]. – Режим доступу: https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf (дата звернення: 04.05.2026).

6. Конвенція про кіберзлочинність від 23.11.2001 [Електронний ресурс]. – Режим доступу: https://rm.coe.int/1680081561 (дата звернення: 04.05.2026).

7. Articles on Responsibility of States for Internationally Wrongful Acts, 2001 [Електронний ресурс]. – Режим доступу: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (дата звернення: 04.05.2026).

8. Report of the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace 2021 [Електронний ресурс]. – Режим доступу: https://undocs.org/A/76/135 (дата звернення: 04.05.2026).

9. UN Open-ended Working Group on ICTs [Електронний ресурс]. – Режим доступу: https://unidir.org/un-open-ended-working-group-and-unidir-side-events/ (дата звернення: 04.05.2026).

10. NATO Cyber Defence Policy [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 04.05.2026).

11. EU Cybersecurity Strategy [Електронний ресурс]. – Режим доступу: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (дата звернення: 04.05.2026).

12. OSCE Confidence-Building Measures in Cyberspace [Електронний ресурс]. – Режим доступу: https://www.osce.org/field-of-work/Cyber-ICT-security (дата звернення: 04.05.2026).

13. UN Digital Cooperation Report [Електронний ресурс]. – Режим доступу: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (дата звернення: 04.05.2026).

14. ICRC. International humanitarian law and cyber operations [Електронний ресурс]. – Режим доступу: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf (дата звернення: 04.05.2026).

15. UNIDIR Cyber Policy Portal [Електронний ресурс]. – Режим доступу: https://cyberpolicyportal.org/ (дата звернення: 04.05.2026).

16. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [Електронний ресурс]. – Режим доступу: 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: 04.05.2026).

17. Hathaway O., Crootof R. The Law of Cyber-Attack [Електронний ресурс]. – Режим доступу: https://www.californialawreview.org/print/law-of-cyber-attack/ (дата звернення: 04.05.2026).

18. Tsagourias N. Cyber Attacks and the Use of Force [Електронний ресурс]. – Режим доступу: https://www.elgaronline.com/monochap/9781786439918.00011.xml (дата звернення: 04.05.2026).

19. Waxman M. Cyber-Attacks and International Law [Електронний ресурс]. – Режим доступу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2926099 (дата звернення: 04.05.2026).

20. Nye J. Cyber Power [Електронний ресурс]. – Режим доступу: https://www.belfercenter.org/publication/cyber-power (дата звернення: 04.05.2026).

21. Rid T. Cyber War Will Not Take Place [Електронний ресурс]. – Режим доступу: https://academic.oup.com/book/12153 (дата звернення: 04.05.2026).

22. Dinniss H. Cyber Warfare and the Laws of War [Електронний ресурс]. – Режим доступу: https://assets.cambridge.org/97811070/11083/frontmatter/9781107011083_frontmatter.pdf (дата звернення: 04.05.2026).

23. Jensen E. Cyber Warfare and LOAC [Електронний ресурс]. – Режим доступу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661218 (дата звернення: 04.05.2026).

24. O'Connell M. Cyber Security without Cyber War [Електронний ресурс]. – Режим доступу: https://scholarship.law.nd.edu/law_faculty_scholarship/1550/ (дата звернення: 04.05.2026).

25. ENISA Threat Landscape Report [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 04.05.2026).

26. Microsoft Digital Defense Report [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report (дата звернення: 04.05.2026).

27. Google Threat Analysis Group [Електронний ресурс]. – Режим доступу: https://blog.google/threat-analysis-group/ (дата звернення: 04.05.2026).

28. World Economic Forum. Global Cybersecurity Outlook [Електронний ресурс]. – Режим доступу: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (дата звернення: 04.05.2026).

29. OECD. Cybersecurity policy making at a turning point: analysing a new generation of national cybersecurity strategies for the Internet economy [Електронний ресурс]. - Paris : OECD Publishing, 2012. - Режим доступу: https://ccdcoe.org/uploads/2018/11/OECD-121116-CybersecurityPolicyMaking.pdf (дата звернення: 04.05.2026)

30. ITU Global Cybersecurity Index [Електронний ресурс]. – Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (дата звернення: 04.05.2026).

31. Конституція України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 04.05.2026).

32. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 04.05.2026).

33. Закон України «Про національну безпеку України» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 04.05.2026).

34. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення: 04.05.2026).

35. Стратегія кібербезпеки України [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 04.05.2026).

36. Cybersecurity and Infrastructure Security Agency. Cybersecurity overview [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/cybersecurity (дата звернення: 04.05.2026).

37. NATO Cooperative Cyber Defence Centre of Excellence. Publications [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/library/publications/ (дата звернення: 04.05.2026).

38. Harvard International Law Journal [Електронний ресурс]. – Режим доступу: https://journals.law.harvard.edu/ilj/ (дата звернення: 04.05.2026).

39. Yale Journal of International Law [Електронний ресурс]. – Режим доступу: https://campuspress.yale.edu/yjil/volume-39/ (дата звернення: 04.05.2026).

40. European Journal of International Law [Електронний ресурс]. – Режим доступу: https://academic.oup.com/ejil (дата звернення: 04.05.2026).

41. Leiden Journal of International Law [Електронний ресурс]. – Режим доступу: https://www.cambridge.org/core/journals/leiden-journal-of-international-law (дата звернення: 04.05.2026).

42. Journal of Conflict and Security Law [Електронний ресурс]. – Режим доступу: https://academic.oup.com/jcsl (дата звернення: 04.05.2026).

43. International Review of the Red Cross [Електронний ресурс]. – Режим доступу: https://international-review.icrc.org (дата звернення: 04.05.2026).

44. Council on Foreign Relations. Cyber operations and international law [Електронний ресурс]. – Режим доступу: https://www.cfr.org (дата звернення: 04.05.2026).

45. Belfer Center for Science and International Affairs. Cybersecurity research [Електронний ресурс]. – Режим доступу: https://www.belfercenter.org (дата звернення: 04.05.2026).

46. NATO Strategic Concept 2022 [Електронний ресурс]. – Режим доступу: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept (дата звернення: 04.05.2026).

47. PlaxidityX. Automotive cyber security company [Електронний ресурс]. - Режим доступу: https://plaxidityx.com/ (дата звернення: 04.05.2026).

48. UN Office for Disarmament Affairs. ICT security [Електронний ресурс]. – Режим доступу: https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context (дата звернення: 04.05.2026).

49. NATO Cyber Threat Assessment [Електронний ресурс]. – Режим доступу: https://www.nato.int (дата звернення: 04.05.2026).

50. World Bank. Digital Development and Cybersecurity [Електронний ресурс]. – Режим доступу: https://www.worldbank.org/en/topic/digitaldevelopment (дата звернення: 04.05.2026).

51. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA) [Електронний ресурс]. – Режим доступу: https://www.icj-cij.org/case/70 (дата звернення: 04.05.2026).

52. Oil Platforms Case (Iran v. USA) [Електронний ресурс]. – Режим доступу: https://www.icj-cij.org/case/90 (дата звернення: 04.05.2026).

53. Kosovo Advisory Opinion [Електронний ресурс]. – Режим доступу: https://www.icj-cij.org/case/141 (дата звернення: 04.05.2026).

54. International Criminal Tribunal for the former Yugoslavia (ICTY) Cases [Електронний ресурс]. – Режим доступу: https://www.icty.org/en/cases (дата звернення: 04.05.2026).

55. International Criminal Court Case Law [Електронний ресурс]. – Режим доступу: https://www.icc-cpi.int/cases (дата звернення: 04.05.2026).

56. Національний інститут стратегічних досліджень. Кібербезпека: світові тенденції та виклики для України [Електронний ресурс]. - Режим доступу: https://niss.gov.ua/sites/default/files/2011-06/kyber_bezpeka-aab17.pdf (дата звернення: 04.05.2026).

57. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» /

Верховна Рада України. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 04.05.2026).

58. Сілін Є. С., Кадубовський О. А. Основи кібербезпеки : навчальний посібник [Електронний ресурс]. - Дніпро, 2023. - 200 с. - Режим доступу: https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf (дата звернення: 04.05.2026).

59. CERT-UA. Реагування на кіберінциденти [Електронний ресурс]. – Режим доступу: https://cert.gov.ua (дата звернення: 04.05.2026).

60. Міністерство цифрової трансформації України [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua (дата звернення: 04.05.2026).

61. RAND Corporation. Cyber Warfare Research [Електронний ресурс]. – Режим доступу: https://www.rand.org/topics/cyber-warfare.html (дата звернення: 04.05.2026).

62. Chatham House. Cyber policy research [Електронний ресурс]. – Режим доступу: https://www.chathamhouse.org (дата звернення: 04.05.2026).

63. Brookings Institution. Cybersecurity studies [Електронний ресурс]. – Режим доступу: https://www.brookings.edu (дата звернення: 04.05.2026).

64. CSIS Cybersecurity Reports [Електронний ресурс]. – Режим доступу: https://www.csis.org/programs/strategic-technologies-program (дата звернення: 04.05.2026).

65. Atlantic Council Cyber Statecraft Initiative [Електронний ресурс]. – Режим доступу: https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/ (дата звернення: 04.05.2026).

66. Carnegie Endowment for International Peace. Cyber policy [Електронний ресурс]. – Режим доступу: https://carnegieendowment.org/programs/technology-and-international-affairs (дата звернення: 04.05.2026).

67. MIT Technology Review. Cybersecurity [Електронний ресурс]. – Режим доступу: https://www.technologyreview.com (дата звернення: 04.05.2026).

68. IEEE Cybersecurity Publications [Електронний ресурс]. – Режим доступу: https://www.ieee.org (дата звернення: 04.05.2026).

69. SpringerLink. Cyber law publications [Електронний ресурс]. – Режим доступу: https://link.springer.com (дата звернення: 04.05.2026).

70. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. [Електронний ресурс]. - Київ : Ліра-К, 2020. - 554 с. - Режим доступу: https://jurkniga.ua/contents/osnovi-kiberprostoru-kiberbezpeki-ta-kiberzakhistu.pdf (дата звернення: 04.05.2026).

71. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник [Електронний ресурс]. - Київ : ДУТ, 2015. - 288 с. - Режим доступу: https://duikt.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 04.05.2026).

72. Gisel L., Rodenhauser T., Dörmann K. Twenty years on: International humanitarian law and cyber operations [Електронний ресурс]. – Режим доступу: https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-10/Twenty-years-on-IHL-and-cyber-operations-final-version.pdf (дата звернення: 04.05.2026).

73. Droege C. Cyber warfare and international humanitarian law [Електронний ресурс]. – Режим доступу: https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf (дата звернення: 04.05.2026).

74. International Review of the Red Cross. International humanitarian law and cyber operations during armed conflicts [Електронний ресурс]. – Режим доступу: https://international-review.icrc.org/articles/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (дата звернення: 04.05.2026).

75. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. [Електронний ресурс]. - Київ : Кондор, 2019. - 272 с. - Режим доступу: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf (дата звернення: 04.05.2026).

76. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual Project [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/research/tallinn-manual/ (дата звернення: 04.05.2026).

77. NATO Cooperative Cyber Defence Centre of Excellence. Cyber Law Toolkit [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/research/cyber-law-toolkit/ (дата звернення: 04.05.2026).

78. European Commission. The EU Cybersecurity Strategy for the Digital Decade [Електронний ресурс]. – Режим доступу: https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-strategy-digital-decade (дата звернення: 04.05.2026).

79. ENISA. ENISA Threat Landscape 2023 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 04.05.2026).

80. Microsoft. Microsoft Digital Defense Report 2023 [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report (дата звернення: 04.05.2026).

81. Кібербезпека : електронний підручник [Електронний ресурс]. - Режим доступу: https://cybersecurity.ptngu.com/ (дата звернення: 04.05.2026).

82. Житомирська політехніка. Основи кібербезпеки : лекція 1 (вибіркова дисципліна) [Електронний ресурс]. - Режим доступу: https://learn.ztu.edu.ua/pluginfile.php/191194/mod_resource/content/4/%D0%9E%D0%9A_%D0%B2%D0%B8%D0%B1%D1%96%D1%80%D0%BA%D0%BE%D0%B2%D0%B0_%D0%BB%D0%BA1.pdf (дата звернення: 04.05.2026).

83. Хвостенко В. С. Правове регулювання кібербезпеки : силабус навчальної дисципліни [Електронний ресурс]. - Харків : НТУ «ХПІ», 2025. - Режим доступу: https://cybersecurity.khpi.edu.ua/wp-content/uploads/2025/12/%D0%A1%D0%9F-7_%D0%9A4_%D0%9F%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%B5-%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B

0%D0%BD%D0%BD%D1%8F-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D0%A5%D0%B2%D0%BE%D1%81%D1%82%D0%B5%D0%BD%D0%BA%D0%BE.pdf (дата звернення: 04.05.2026).

84. Інститут інформації, безпеки і права НАПрН України. Правове забезпечення кібербезпеки : робоча навчальна програма [Електронний ресурс]. - Київ, 2024. - Режим доступу: https://ippi.org.ua/sites/default/files/rnp_pravove_zabezpechennya_kiberbezpeki_2024.pdf (дата звернення: 04.05.2026).

85. RAND Corporation. Cyber Warfare: Understanding National Security in a Digital Age [Електронний ресурс]. – Режим доступу: https://www.rand.org/pubs/research_reports/RR1600.html (дата звернення: 04.05.2026).

86. Atlantic Council. The Cyber Statecraft Initiative [Електронний ресурс]. – Режим доступу: https://www.atlanticcouncil.org/programs/cyber-statecraft-initiative/ (дата звернення: 04.05.2026).

87. KPMG. Cyber considerations [Електронний ресурс]. - 2022. - Режим доступу: https://assets.kpmg.com/content/dam/kpmgsites/ua/pdf/2022/03/KPMG-cyber-considerations.pdf (дата звернення: 04.05.2026).

88. Center for Strategic and International Studies. Significant Cyber Incidents Timeline [Електронний ресурс]. – Режим доступу: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (дата звернення: 04.05.2026).

89. Кібербрама. Кібербезпека під час війни [Електронний ресурс]. - Режим доступу: https://stopfraud.gov.ua/cybersecurity-in-wartime (дата звернення: 04.05.2026).

90. NATO. Cyber Defence [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 04.05.2026).