МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
Кафедра міжнародного права та порівняльного правознавства

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

_____ Р. О. Максимович
«____»_____2023 р.

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

«МАГІСТР»

спеціальності 293 «Міжнародне право»

ТЕМА: КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА МІЖНАРОДНІЙ ТА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ: ПРАВОВИЙ АНАЛІЗ ТА ПИТАННЯ РЕАЛІЗАЦІЇ

Виконавець: Якубенко Наталія Андріївна
Науковий керівник: к.ю.н. Замула Аліна Юріївна
Нормоконтролер: викладач Головатенко Марина Юріївна

Київ, 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АФ – Африканський союз

ГА ООН – Генеральна Асамблея Організації Об’єднаних Націй

ЄС – Європейський союз

ІКТ – Інформаційно-комунікаційні технології

КНР – Китайська Народна Республіка

ЛАД – Ліга арабських держав

НАТО – Організація Північноатлантичного договору

ОБСЄ – Організація з безпеки та співробітництва в Європі

ООН – Організація Об’єднаних Націй

РЄ – Рада Європи

СНД – Співдружність Незалежних Держав

США – Сполучені Штати Америки

ШОС – Шанхайська організація співробітництва

ВСТУП

Актуальність теми. У сучасному світі, охопленому безпрецедентним розвитком технологій та глибокою цифровою взаємодією, кіберзлочинність стає зростаючим викликом для міжнародної спільноти. Вона представляє собою не традиційний вид правопорушення, а досить молоде явище, яке пов'язане із появою та поширенням глобальної мережі Інтернет. Унікальна природа Всесвітньої мережі забезпечила її користувачам глобальне охоплення та анонімність, що стало передумовою для появи даного виду злочинності. З поширенням кіберзлочинів виникла потреба в правовому регулюванні цього питання як на міжнародному рівні, так і в Україні.

Протидія будь-якому негативному впливу передбачає формування розуміння суті проблеми та усвідомлення її походження. З урахуванням того, що швидкість розвитку суспільства тісно пов'язана із досягненнями науково-технічного прогресу та проявами злочинності, важливим є також вивчення розвитку впровадження правових механізмів для протидії кіберзлочинності як у світі, так і в Україні. Злочинні дії у кіберпросторі охоплюють широкий спектр загроз, від крадіжок особистої інформації до суттєвих атак на критичну інфраструктуру країн. У цьому контексті важливо розглядати міжнародні правові аспекти кіберзлочинності, оскільки технологічні виклики перетинають межі національних держав, вимагаючи гармонізації законодавства та ефективного міжнародного співробітництва.

Кіберзлочинність, що спостерігається в сучасному інформаційному суспільстві, відзначається своєю новизною та постійними змінами, пов'язаними із стрімким розвитком технологій. Злочинці не лише використовують інновації, але й активно адаптують їх для здійснення кримінальних дій, створюючи виклик для правових систем та міжнародного співтовариства.

Аналіз наукового досвіду у сфері вивчення кіберзлочинності свідчить про те, що на сучасному етапі це питання залишається недостатньо

розглянутим. Дослідження обмежуються певними аспектами, а сам термін «кіберзлочинність» ще потребує чіткого визначення та розробки єдиної системи боротьби. У цьому контексті важливо розвивати наукові підходи та виробляти нові стратегії, щоб ефективно протистояти цьому складному явищу.

Для України та світу загалом, виникає необхідність у створенні універсальних стандартів та стратегій протидії кіберзлочинності, що враховуватимуть не лише сучасні реалії, але й прогнозовані технологічні та соціокультурні тенденції. Наукова спільнота, разом із правоохоронними органами, повинна активно сприяти цьому процесу, забезпечуючи стійкий розвиток міжнародного правового регулювання та вдосконалення інструментів боротьби із кіберзлочинністю.

Міжнародні норми та договори до сьогоднішнього дня відображають лише обмежену спроможність відповідати на виклики кіберзлочинності, адаптуватися до нових загроз та забезпечувати належний рівень захисту. Аналіз законодавства та вивчення міжнародного досвіду щодо протидії кіберзлочинності стає ключовим етапом розроблення ефективних стратегій та політик, призначених для покращення міжнародного співробітництва та зміцнення правового врегулювання в цьому напрямку.

Актуальність теми міжнародної боротьби з кіберзлочинністю беззаперечна в умовах швидкого технологічного прогресу та все більшої залежності суспільства від цифрових технологій. Зростання кількості та складності кіберзагроз, спрямованих як на окремих громадян, так і на важливі національні та міжнародні інфраструктурні об'єкти, створює нагальну необхідність вдосконалення правового реагування на ці виклики.

Кіберзлочинність вже давно перейшла кордони традиційного злочину, але поточні міжнародні норми та угоди не завжди здатні ефективно реагувати на нові та вдосконалені методи кіберзлочинців. Зокрема, низка подій, таких як масштабні атаки на інформаційні системи країн, підкреслює

потребу у глибокому аналізі та удосконаленні міжнародних підходів до кібербезпеки та правопорядку.

Актуальність цієї теми також полягає в необхідності пошуку балансу між забезпеченням безпеки та захистом особистих прав та свобод громадян у цифровому просторі. Розвиток ефективних стратегій та міжнародного співробітництва в цій області є ключовим завданням для забезпечення стійкості та безпеки сучасного суспільства в умовах цифрової епохи.

В умовах стрімкого розвитку технологій та поширення кіберзагроз, стає очевидним, що існуючі методи боротьби з кіберзлочинністю стають застарілими. Потрібна не просто модернізація, але й повний реінжиніринг системи захисту. У цьому контексті, важливо визначити та розглянути новаторські підходи, спрямовані на вдосконалення кібербезпеки.

Інтеграція штучного інтелекту та машинного навчання може виявитися ключовою стратегією в протидії кіберзлочинності. Системи, які можуть аналізувати величезні обсяги даних та прогнозувати нові види загроз, відкривають нові перспективи для попередження кібератак та реагування на них швидше, ніж коли-небудь.

Паралельно з технічними інноваціями, важливо приділяти увагу людському фактору в кіберзахисті. Збільшення рівня свідомості користувачів, навчання їх визначати та запобігати соціальному інженерінгу може стати ефективним бар'єром для численних кіберзагроз. У реальному часі обмін інформацією та співпраця між країнами стає визначальною у глобальній боротьбі з кіберзлочинністю. Важливо також звернутися до етичних питань, пов'язаних із застосуванням нових технологій в кібербезпеці. Забезпечення прав та свобод громадян у цифровому просторі, врахування приватності та прозорості, може стати фундаментальними принципами розвитку кібербезпеки.

У відповідь на динамічні кіберзагрози, необхідно розглядати боротьбу з кіберзлочинністю як постійний процес, що вимагає постійного

вдосконалення та адаптації. Створення гнучких та реактивних стратегій може допомогти суттєво зменшити вразливість перед сучасними кіберзагрозами.

Мета і завдання дослідження. Мета цього дослідження полягає в глибокому аналізі міжнародних правових аспектів кіберзлочинності та висвітленні недоліків та викликів, які виникають при впровадженні ефективних стратегій протидії цьому явищу.

На основі визначеної мети було поставлено ряд завдань:

– розглянути кіберпростір як сферу глобальних конфронтацій;

– проаналізувати понятійно-категоріальне осмислення кібербезпекової політики;

– дослідити поняття, сутність та ознаки кіберзлочинності в міжнародному праві;

– визначити правове регулювання боротьби та співробітництва в питаннях кіберзлочинності;

– розглянути виклики та перспективи боротьби з кіберзлочинністю.

Об'єкт дослідження – кіберзлочинність в контексті міжнародних правових відносин та співробітництва.

Предмет дослідження – міжнародні правові аспекти кіберзлочинності аналіз законодавства та пропозиції щодо покращення міжнародного співробітництва.

Методологічна основа дослідження. У даному дослідженні використовуються різноманітні методи для глибокого аналізу міжнародних правових аспектів кіберзлочинності та виявлення можливостей для покращення міжнародного співробітництва. Правовий аналіз ґрунтується на ретельному вивченні чинного законодавства, угод та конвенцій. Порівняльний аналіз дозволяє виявити спільні підходи та різницю у регулюванні кіберзлочинності в різних країнах.

Документальний аналіз ґрунтується на вивченні наукових праць, доповідей та законодавчих ініціатив з проблеми дослідження. Метод кейс-стаді використовується для вивчення конкретних випадків міжнародної

реакції на кіберзлочинність. Цей комплексний підхід дозволяє систематично дослідити та зрозуміти проблематику кіберзлочинності, а також надати конкретні пропозиції для вдосконалення міжнародної співпраці у цьому напрямку.

Структура та обсяг дипломної роботи. Структура дипломної роботи зумовлена предметом, метою та завданнями дослідження. Дипломна робота складається із переліку умовних скорочень, вступу, трьох розділів, якими охоплюються сім підрозділів, висновків та списку використаних джерел (86 найменувань). Загальний обсяг дипломної роботи _ сторінки, у тому числі список використаних джерел – 91 сторінка.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ КІБЕРПРОСТОРУ, КІБЕРЗЛОЧИННОСТІ ТА КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ

1.1. Кіберпростір як сфера глобальних конфронтацій

Кіберпростір утворює сферу глобальних конфронтацій, де відбуваються різноманітні дії – кібератаки, кібершпигунство, інформаційна війна та кіберзлочинність. Держави, корпорації та групи використовують цей простір для досягнення економічних, політичних та військових цілей. Забезпечення кібербезпеки та розробка міжнародних норм стають надважливими завданнями для формування стабільності та безпеки в цифровому середовищі [33, с.19].

Сучасна людина активно використовує інформаційно-комунікативні технології, які є унікальними для нашого часу. Розвиток цих технологій спричинив введення у науковий дискурс таких понять, як: «віртуальна реальність», «кіберпростір» і «мережеве суспільство». Концепт «кіберпростір» визначає новий аспект реальності, який став ключовим фактором соціокультурного середовища. Це особливий простір, який взаємодіє з усіма сферами суспільного життя – економічною, соціальною, політичною та духовною.

Термін «кіберпростір» відкриває перед нами різноманітні аспекти, наприклад:

– область взаємодії між особами, програмами та сервісами у величезній мережі Інтернет за допомогою технічних пристроїв та комунікацій, яка не обмежена фізичною формою;

– сфера, де використання електронних та електромагнітних засобів дозволяє запам'ятовування, модифікацію та обмін даними через системи, що працюють у мережі Інтернет і пов'язана з фізичною інфраструктурою;

– всі аспекти мережевої та цифрової активності, які включають контент і операції з їх обробки;

– інформаційна структура, доступна через глобальну мережу;

– середовище комунікації, що формується системою взаємозв'язків між об'єктами цифрової інфраструктури, серед яких вирізняються: електронні обчислювальні системи, комп'ютерні мережі, програмне забезпечення та інформаційні ресурси .

З урахуванням наукових характеристик кіберпростору важливо визначити його як кіберінформаційне середовище, що складається з інформаційної інфраструктури та взаємозв'язків між цими об'єктами. Інформаційна інфраструктура включає різноманітні об'єкти, такі як: гаджети, комп'ютери, комп'ютерні мережі, пристрої та програмно-технологічні компоненти.

Використання префікса «кібер-» вказує на пов'язаність всіх інформаційних баз із науковим аналізом, їх обґрунтованість з погляду суспільної ефективності та необхідності, а також дослідження аспектів збереження, авторизації та захисту інформації з метою збереження авторських прав і захисту честі, гідності та ділової репутації в інформаційних мережах. Також, це може сприяти формуванню нового механізму взаємодії в межах кіберкультури.

Крім того, виникнення кіберпростору сприяло формуванню глобального інформаційного простору та розвитку «мережевого суспільства». Основою його функціонування є генерація, обробка, передача та оновлення інформаційного соціокультурного поля. Кіберпростір впливає на спілкування сучасної людини, формує її повсякденний досвід і визначає її поведінку [37, с.98].

Багато з великих світових держав, таких як США, Китай та Індія, на даний момент активно розробляють і трансформують свої військові кібернетичні підрозділи, спрямовуючи їх на використання можливостей Інтернету для захисту національних інтересів та здатність впливати на інші

країни. Наприклад, у США створено військову кіберкоманду (U.S. Cyber Command), а Великобританія, Німеччина, Австралія, Індія, Ізраїль також вже мають власні кібервійськові підрозділи [37, с.99].

Зокрема, ці військові кіберпідрозділи відзначаються активною захисною діяльністю. У світі також існують різні міжнародні безпекові організації, зокрема НАТО та ОБСЄ, які вживають заходів для протидії кіберзагрозам. Такий підхід свідчить про зростаюче прагнення провідних держав захищати свої інформаційні ресурси та мати змогу впливати на інші інформаційні ресурси [37, с.88].

Це підтверджується бажанням регулювати питання стосовно визнання кібератак, як актів війни, на міжнародному рівні. Експерти в області кібербезпеки вважають військові кіберпідрозділи Китаю та США найпотужнішими та найактивнішими. Інформації про потенціал, чисельність і завдання китайських кібервійськ практично немає, проте доктринальні безпекові документи КНР вказують на зростання ролі інформатизації у військовій справі ще з середини 90-х років минулого століття.

У Білій книзі з питань оборони 2008 року визначалася амбіційна мета досягнення значних результатів у справах інформатизації армії Китаю до 2020 року. Проблемі розбудови інформаційного потенціалу збройних сил КНР приділялася велика увага і в Білій книзі з питань оборони 2010 року [32, с.155].

У Стратегії національної безпеки США 2010 року вперше відділили окремий розділ про кіберзагрози. Для подальшого розвитку кіберпростору США визначили Міжнародну стратегію для кіберпростору. У 2011–2012 роках було прийнято кілька практичних документів, спрямованих на зменшення кіберзагроз, зокрема щодо протидії бот-мережам і кібершпигунству.

Президент Б. Обама, 5 січня 2012 року, оголосив про зміни в оборонній стратегії, де чітко було вказано, що видатки на кібербезпеку не тільки не зменшаться, але й збільшаться, навіть при зменшенні загальних видатків на

оборону. Це рішення підтверджує думку про те, що кібербезпека була, є і буде критичною для майбутніх успіхів США [51].

Важливо розуміти, що розвиток інформаційних технологій, з того часу, суттєво пішов вперед, впливаючи на всі сфери життя. Зростання кількості підключених до Інтернету пристроїв та об'ємів цифрової інформації створює нові виклики для безпеки та взаємодії в кіберпросторі. В умовах такого постійного технологічного розвитку, необхідно враховувати, що кіберпростір стає важливим інструментом впливу в політичних конфліктах, впливаючи на перебіг подій та визначаючи стратегії держав і політичних груп.

Політичні конфлікти пройшли різні етапи розвитку, впливаючи своєю діяльністю на розвиток та благополуччя суспільства. У сфері інформаційних технологій та систем, суспільство ще не досягло значного рівня розвитку, іноді у звичайних політичних конфліктах пересічному громадянину складно розібратись та надати об'єктивну оцінку конфліктним процесам. В кіберпросторі виникає фантомне уявлення про відсутність будь-якого впливу на пересічних мешканців суспільства. Тим не менше, важливість конфліктної активності в кіберпросторі між впливовими політичними акторами є глобально небезпечною та катастрофічно орієнтованою [18, с.96].

Політичні конфлікти розгортаються в межах кіберінформаційного середовища, де його ознака публічності та відкритості активно обговорюється та коментується різними особами. З одного боку, багато активних користувачів в Інтернеті не такі активні в реальному політичному житті та прийнятті політичних рішень [18, с.96]. Наприклад, виборчий процес обговорюється на різних сайтах та на сторінках політиків, але значна частина потенційних виборців не звертається до виборчих дільниць для підтвердження своєї політичної позиції. З іншого боку, політичні конфлікти в кіберпросторі можуть мати небезпечні наслідки, такі як: кібератаки та хакерські дії, спрямовані на підрив державних інтересів та політичної системи в цілому.

Отже, крім розгляду кіберпростору як сфери глобальних конфронтацій, важливо розглядати питання кібербезпеки як необхідного компоненту формування інформаційної політики в сучасній країні. За поглядами О.Ткаченко та К.Ткаченко, кібербезпека визначається як стан захищеності кіберпростору держави від можливих кібервпливів, які можуть порушити стабільний або сталий розвиток [73, с.76]. Це включає в себе виявлення загроз, запобігання та ефективну нейтралізацію кіберзлочинів, які становлять загрозу особистим, корпоративним та національним інтересам.

Коли дії окремих суб'єктів політики можуть визнатися як кібератака чи кіберзлочин в контексті політичних протиріч, вони потрапляють під механізм дій, спрямованих на забезпечення кібербезпеки інформаційних систем. Таким чином, при низькому рівні кібербезпеки держави, політичне протиріччя в кіберпросторі стає неконтрольованим і існуючі механізми впливу на політичні конфлікти стають неефективними. У такому випадку політичний конфлікт може розширюватися до глобальних масштабів та впливати на політичні процеси у всьому світі, а також на фінансові показники та розвиток економіки в різних країнах.

З урахуванням актуальності цього питання на міжнародному рівні, кожна країна світу має необхідність створення національних основ для захисту інформаційного середовища з метою вироблення національної системи безпеки в межах кіберпростору. Крім того, прийняття нормативно-правових механізмів впливу може сприяти створенню основного захисту з метою зменшення кіберконфліктів та прямих політичних атак, наслідки яких на даний момент переживають пересічні громадяни [78].

Для більш глибокого розуміння атак необхідно розробляти новітні методи, які сприятимуть захисту інформаційних систем окремих сфер та забезпечать стійкий захист, попереджаючи потужні агресивні напади в інформаційному просторі. Відповідно до думки В.С. Цимбалюка, кіберпростір представляє собою сегмент віртуального середовища, де можливість здійснення комунікацій у суспільних відносинах реалізується

через функціонування взаємопов'язаних технічно та технологічно електронних інформаційних систем, таких як Інтернет та/або інші комп'ютерні мережі передачі даних, з метою управлінського впливу [78].

Враховуючи це, можна зазначити, що розвиток кіберпростору відкриває нові можливості, але одночасно породжує нові виклики, зокрема в сфері кібербезпеки. Одним із таких викликів є поняття кібервійни, яке в сучасному світі виявляється як необхідний аспект інформаційної безпеки.

На сьогодні кібервійна виступає невід'ємною складовою інформаційної боротьби, що діє як додатковий, але ефективний інструмент психологічного тиску на опонента. З урахуванням стрімкого розвитку та удосконалення інформаційних технологій, кібервійна досягла рівня класичних конфліктів і вона радикально змінює стратегію ведення війни.

Доцільно відзначити, що трактувань відносно терміну «кібервійна» є багато, але основними елементами виступають:

1) скоординовані цифрові (кібер) атаки однієї держави на комп’ютери та мережі іншої держави з метою завдання шкоди чи руйнування;

2) конфлікт, який передбачає використання ворожих, незаконних атак на комп’ютери та мережі для руйнування комунікацій та інфраструктури для завдання економічної шкоди чи підриву системи оборони країни;

3) використання комп’ютерних технологій та мереж Інтернет державою або за її підтримки проти іншої держави з метою порушення її безпеки та оборони, що становить серйозну загрозу для її суверенітету [71, с.21].

Особливості кіберпростору, як середовища ведення цифрової (кібер) війни, породжують специфічні риси цифрового конфлікту, які можна визначити за допомогою емпіричних методів дослідження. По-перше, в цифровому протистоянні неможливо ідентифікувати «агресора», навіть якщо причетність державних структур певних країн до цифрових атак здається очевидною. По-друге, характерною ознакою цифрового (кібер) конфлікту є прихованість впливу і відсутність видимих руйнувань. Виявити початок кібер атаки, вжити превентивні заходи для запобігання таким атакам, а також

адекватно оцінити рівень загрози і масштаб завданих збитків дуже складно. По-третє, цифровий (кібер) конфлікт характеризується надзвичайною швидкістю проведення атак, коли час між початком «агресії» та її наслідками скорочується до мінімуму [63, с.339].

По-четверте, шкідливі програми володіють здатністю швидкого «розмноження» шляхом створення копій і майже безперешкодного розповсюдження в різних мережах. По-п'яте, для кіберзброї не існує кордонів та відстаней і часто відсутні не лише технологічні, але й юридичні перешкоди для проникнення в комп'ютерні системи та мережі супротивника, що дозволяє віддалено управляти його ресурсами.

Кіберінциденти важко контролювати з боку державних служб розвідки та безпеки. На відміну від традиційної зброї, кіберозброя не обов'язково знищує об'єкт впливу, а, навпаки, впроваджує певний набір даних і команд, які змінюють (або порушують) існуючі алгоритми функціонування системи. Суттєвою особливістю кіберпротистояння є її відносна незавершеність, оскільки учасники протистояння не можуть бути впевнені в припиненні атак.

Кібервійна спрямована передусім на дестабілізацію комп'ютерних систем і доступу до Інтернету державних установ, фінансових і ділових центрів, а також на створення безладу і хаосу в житті країн, які значно покладаються на Інтернет у повсякденному житті. Таким чином, в епоху інформаційної революції досягнення політичних цілей не обов'язково вимагає введення військ, окупації, захоплення територій чи величезних військових витрат [47, с.35].

Зброя «мережі», що представляє новий четвертий простір після суходолу, моря та повітря, стає зручнішою. Оскільки Інтернет об'єднує практично весь світ, атака на мережу однієї держави може призвести до атаки на інші. Отже, міждержавні відносини та політичне протистояння знаходять своє відображення та втілення в інтернеті у формі кібервійни.

1.2. Понятійно-категоріальне осмислення кібербезпекової політики

У галузі кібербезпеки виникає корінний вплив бінарної природи основних концепцій. З одного боку, процес глобалізації світу та присутність кіберпростору перетинають традиційні межі та обмеження щодо джерел інформації, утворюючи транснаціональний елемент для незаконних дій у сфері інформаційних технологій. Це призводить до усвідомлення масштабів єдиного кібернетичного простору та відповідальності кожної держави перед світовою спільнотою [7, с.24].

З іншого боку, національна безпека залишається ключовою функцією будь-якої держави, визначаючи необхідність розробки, впровадження та постійного вдосконалення системних управлінських, економічних та технологічних заходів для забезпечення кібербезпеки. Концепція впровадження кібербезпекової політики ефективно вирішує ці завдання. Важливо враховувати, що формування концептуальної сфери кібербезпекової політики включає різнобічні та різновекторні стратегії.

Кібербезпекова політика визнається однією з пріоритетних галузей сучасної державної діяльності. Виникнення цього напрямку обумовлене стрімким розвитком технологій та проникненням інформаційних технологій у всі сфери життєдіяльності. Регулювання цього сегменту стає надзвичайно актуальним внаслідок зростання реальних загроз для окремих громадян, організацій, установ, закладів і держави в цілому [3, с.55].

Державну політику можна розглядати як напрямок дій чи бездіяльності, який обирає державна влада або орган державної влади з відповідними повноваженнями (правовими, політичними, інформаційними та фінансовими) для вирішення конкретних проблем або сукупності взаємозалежних проблем [16, с.142].

Таким чином, з позиції реактивного підходу державна політика може бути сприйнята як відповідь держави на конкретні проблеми суспільства чи

груп у суспільстві, таких як громадяни та неурядові організації. Вона взаємодіє з різними соціальними групами, формує механізми балансу та консенсусу для забезпечення стабільності та розвитку суспільства. У контексті кібербезпеки, державна політика повинна бути спрямована на вирішення конкретних проблем, що виникають у кіберпросторі. Оскільки питання кібербезпеки тісно пов'язані із загальною безпекою, для проведення дослідження ми будемо використовувати основні нормативно-правові акти у сфері безпекознавства [29, с.217].

Виходячи з аналізу останніх років, керівництво держави прийняло ряд вагомих дій, які націлені на боротьбу з кіберзагрозами та покращення національної системи кібербезпеки. Так, у Законі України «Про національну безпеку України» [56] задекларовано положення, що національна безпека України забезпечується через виважену державну політику без обмеження конкретних аспектів, таких як економічна, соціальна, інформаційна чи кібернетична сфери. Даний нормативно-правовий акт зосереджується на державній політиці як на провідному інструменті формування сприятливих та якісних умов в питаннях безпечного та стабільного функціонування суспільства та держави.

Вважаємо необхідним провести уточнення поняття «державна політика кібербезпеки». Для цього можна адаптувати тлумачення поняття «державної політики національної безпеки», яке було введене в науковий обіг В.А. Ліпканом та О.С. Ліпкан [45, с. 85]. За їх поглядами, «державна політика кібербезпеки» має розглядатись як діяльність уповноважених органів державної влади і управління, яка визначає мету, пріоритетність, принципи, функції, способи, методи та засоби забезпечення кібербезпеки [45].

Через те, що державна політика кібербезпеки визначається як складовий блок інформаційної політики, можна виокремити два основні взаємопов’язані структурні елементи, зокрема:

1) діяльність виключно державних органів;

2) діяльність недержавних інституцій, представників громадянського та інформаційного суспільства в інформаційній сфері [45].

Роблячи аналіз норм Закону України «Про національну безпеку України», доцільно зробити акцент на державній політиці, що здійснюється від імені держави її владними органами. Саме через те, що державні органи володіють інструментами державного примусу, їх часто пов'язуються із термінами «захист», «безпека», «охорона» [56]. Таким чином, державна політика кібербезпеки включає в себе засоби захисту, охорони та забезпечення безпеки.

Проводячи аналіз кібербезпекового законодавства, необхідно обов'язково застосовувати формально-юридичний та логіко-семантичний аналіз текстів, щоб виокремити поняття «кібероборона», «кібернапад», «кібербезпека», «кіберзахист». Це необхідно робити, адже в науковому дискурсі часто дослідники можуть ці слова розглядати як синоніми та застосовувати у своїх працях без чітких розмежувань. На нашу думку, це є неприпустимим, адже всі терміни хоча і пов'язані з кіберпростором та його викликами, все ж вони різні за своєю сутністю та змістовним наповненням [54, с.91].

Потреба у виборі альтернативних засобів, методів і шляхів для забезпечення кібернетичної безпеки визначається характером і розмірами загроз національним інтересам у різних сферах життєдіяльності. Зазначимо, що стратегія державної політики в галузі кібербезпеки має базуватися на принципах реалізації національних інтересів та враховувати цінності демократії та принципу верховенства права.

На прикладі України можемо відзначити, що згідно із Законом України «Про національну безпеку України», наявні дві основні категорії, якими визначено змістовне спрямування державної політики кібернетичної безпеки. До них, зокрема, варто віднести:

1) загрози національним інтересам та національній безпеці держави в кібернетичній сфері.

2) основні напрями державної політики з питань національної безпеки в кібернетичній сфері [56].

Проводячи аналіз думок В.А. Ліпкана [45], а також беручи до уваги вагомість аспектів кібербезпеки як складової інформаційної безпеки, можна здійснити адаптацію цих ідей до вивчення обраної теми. Таким чином, сучасна галузь державної політики в сфері кібербезпеки визначає впровадження державних заходів у кіберпросторі. Основною ціллю цієї діяльності є задоволення інформаційних потреб громадян та формуванні відкритого інформаційного суспільства, відомого також як кіберсуспільство. Це передбачає не лише розвиток єдиного кіберпростору країни, але й її активну інтеграцію в світовий кіберпростір, з урахуванням збереження національної ідентичності та реалізації національних інтересів на внутрішній та міжнародній аренах.

Основною метою державної політики в галузі кібербезпеки є керування реальними та потенційними кібервикликами з метою створення необхідних умов для задоволення інформаційних потреб громадян та реалізації національних інтересів у цьому контексті [70, с.156].

Важливим аспектом є те, що не всі чинні нормативно-правові акти відповідають сучасним викликам, загрозам та відповідають реальному часу. В більшій мірі прийняття нових законодавчих актів суттєво затримується або швидко застаріває та не відповідає вимогам сучасного розвитку суспільства.

Ми погоджуємося з позицією І.В. Арістової, яка звертає увагу на доцільності зміни та переформатуванні пріоритетів державної політики, виробленні нових концепцій щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної стратегії, а також розвитку інформаційного законодавства для ефективного забезпечення інформаційної безпеки [2, с.58].

Щодо конкретних напрямків державної політики у галузі кібербезпеки, акцент робиться на її чіткому визначенні та закріпленні в національному законодавстві. Вже зараз активно ведеться розробка змін до Закону України

«Про основні засади забезпечення кібербезпеки України», щоб врахувати всі нові виклики, які стають актуальними зі зміною динаміки інформаційних політик в світі [57, с.371].

В даному нормативно-правовому акті, напрями державної політики закріплені так:

– необхідність формування захищеного національного сегменту кіберпростору. Цей напрям націлений на формування відкритого суспільства, що дасть можливість використовувати кіберпростір безпечно. Варто наголосити, що дефініція «відкрите суспільство» можна вважати відносно новою в науковому дискурсі. Таке суспільство має базуватись на плюралізмі і визнанні прав та інтересів всіх, без виключення, громадян.

– Супротив втручанню у внутрішню політику держави та нейтралізація посягань на її інформаційні ресурси з боку інших держав.

– Підкріплення позицій щодо обороноздатності держави, зокрема в продумуванні механізмів кібероборони.

– Боротьба з кіберзлочинністю та кібертероризмом. Необхідно детально розмежувати суб'єктів цього напряму, які бедуть нести відповідальність, оскільки кіберзлочинність стала актуальною проблемою, яка суттєво збільшується та масштабується, приносить збитки.

– Зменшення уразливості об'єктів кіберзахисту, особливо об'єктів критичної інформаційної інфраструктури. Цей напрям повинен виробити нові підходи до тлумачення та закріплення дефініції «об'єкт кіберзахисту», адже ця категорія малодосліджена. Поняття «зменшення уразливості» залишається абстрактним без чіткої методики визначення та критеріїв.

– Забезпечення повноправної участі держави не лише в європейському просторі, а й в регіональних системах забезпечення кібербезпеки. Заборона чи обмеження участі України лише в межах єдиного простору своєї держави є некоректним через те, що система забезпечення кібербезпеки має включати широке коло суб'єктів та масштабність дій.

– Дотримання міжнародних зобов'язань в питаннях боротьби з кіберзлочинністю та кібертероризмом та їх запобіганню. На сьогодні існує обмежена кількість нормативно-правових актів, у яких держави зобов'язуються боротися з кібертероризмом та кіберзлочинністю на світовому рівні через міжнародній співпрацю. Проте, ратифікація Конвенції про кіберзлочинність є прикладом такого зобов'язання та визначає необхідність приведення національного законодавства у відповідність із рекомендаціями цього міжнародного документу [57].

Оскільки кібербезпека входить у склад інформаційної безпеки, яка, в свою чергу, становить частину національної безпеки, розумним буде адаптація положень Закону України «Про основи національної безпеки України» до загальноєвропейських норм, що є важливим при формулюванні напрямків державної політики з кібербезпеки.

1.3. Поняття, сутність та ознаки кіберзлочинності в міжнародному праві

Кіберзлочинність – це одна з основних та стрімко зростаючих загроз у сучасному правоохоронному середовищі, що викликає підвищений інтерес розвинених країн. Цей інтерес обумовлений, зокрема, поширеністю кіберправопорушень [15].

Термін «кіберзлочинність» вперше виник у американській літературі на початку 1960-х років і передбачав порушення прав та інтересів, які були пов’язані із системами автоматизованої обробки даних. Джон Дрейпер ввійшов в історію як перший кіберзлочинець, який влився в злочинну діяльність у 1970-х роках. Дрейпер отримав прізвисько «телефонний хакер» через свою діяльність по взлому телефонних мереж. Історичний арешт кіберзлочинців, який вперше було здійснено, стався в 1983 році в Мілуокі. Тоді злочинцями були підлітки, які зробили незаконне проникнення 60 комп'ютерів. В справі підлітки фігурували як «група 414» [23].

Проте, необхідно відзначити, що на сьогодні відсутнє загальноприйняте визначення кіберзлочинності не лише на міжнародному, а й на національному рівні [36, с.173]. Поняття цього явища в процесі міжнародно-правового регулювання постійно розширюється та уточнюється. Розробка міжнародно-правової концепції кіберзлочинності повинна базуватися на уніфікованому визначенні терміну «кіберзлочин» та однакових підходах до криміналізації цього виду протиправних дій [21, с.131]. Уніфікація міжнародно-правових норм у протистоянні кіберзлочинності є ключовим засобом розвитку галузі міжнародного кримінального права і необхідною частиною загальної уніфікації міжнародного права в умовах глобалізації.

У Великому українському юридичному словнику термін «кіберзлочинність» описується як сукупність порушень закону, що трапляються в рамках комп'ютерної системи чи мережі електрозв'язку з використанням комп'ютерної мережі [12].

Згідно з означенням С.Г.Каланча, це представляє собою соціально-правовий явище, проявляється у забороненій кримінальній діяльності частини населення за допомогою електронно-обчислювальних машин, телекомунікаційних систем та комп'ютерних мереж [38, с.215]. Визначення Т.Л. Сироїд вказує на те, що кіберзлочинність – це явище, що виявляється у системі злочинів, скоєних в кіберпросторі з використанням чи проти комп'ютерних даних, мереж та інших телекомунікаційних систем, включаючи Інтернет та технології мобільного зв'язку [66, с.195].

Незважаючи на відсутність єдності визначень кіберзлочинності, вчені в кримінології також не досягли консенсусу щодо термінів, які можуть використовуватися для позначення цього явища. Окрім «кіберзлочинності», вживаються такі терміни, як «комп'ютерна злочинність», «злочини у сфері високих технологій», «інформаційні злочини», «злочини у сфері комп'ютерної безпеки» тощо. У вітчизняній кримінології переважає використання терміну «комп'ютерна злочинність» як синоніму для

«кіберзлочинності». Тим не менш, існують підходи, які розглядають кіберзлочинність як більш широке поняття, ніж «комп'ютерна злочинність», охоплюючи різні форми злочинності, де комп'ютер може бути знаряддям чи способом для злочинів проти власності, авторських прав, громадської безпеки, моралі і т.д.

Ознаками, що визначають кіберзлочинність як злочин міжнародного характеру, є збільшена суспільна небезпека через порушення порядку та режиму існування інформації, доступ до якої відбувається за допомогою електронно-технічних засобів [46, с.86]. Це підтверджується значною вразливістю національних і міжнародних правопорядків перед цією формою злочинної діяльності, обмеженими можливостями держав і міжнародного співтовариства в попередженні, контролі та протидії таким злочинам, а також можливістю завдання значної шкоди кіберзлочинністю.

Сфера високих технологій в цілому характеризується значними фінансовими витратами, і злочинні втручання в ці технології створюють суспільну небезпеку цієї категорії злочинів. Крім того, важливим є співвідношення між витратами на підготовку та вчинення злочинів і їхніми наслідками [30].

Економічний компонент кіберзлочинності суттєво визначається матеріальною шкодою. Це охоплює різноманітні види протиправних дій, включаючи порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем. Такі правопорушення дозволяють злочинцям користуватися обмеженими даними, що може призвести до оприлюднення інформації майнового та немайнового характеру, погіршення іміджу та завдання інших збитків.

Зловживання, пов'язані з комп'ютерами, непрямо завдають шкоду через такі прояви, як крадіжки коштів, шахрайство та інші аспекти. У контексті інформації також спостерігається економічний інтерес, наприклад, оплата за отримання відповідної інформації. Зазвичай розрахунки здійснюються анонімно, а кошти акумулюються і використовуються без контролю, роблячи

підприємницьку діяльність повністю «тіньовою». В порушенні авторських та суміжних прав вже давно визнається злочин економічного характеру через існування «піратського» бізнесу на міжнародному рівні. Транснаціональний характер таких протиправних дій підкреслює можливість їх здійснення з територій різних держав або з тих, де режим протидії недостатньо розвинений. Злочинців приваблює відсутність фізичного контакту з потерпілими, складність виявлення та вилучення криміналістично-значущої інформації у віртуальному просторі [49, с.250].

З огляду на ці умови виникають відповідні міжнародно-правові зобов'язання у міжнародному праві, які вимагають удосконалення національного законодавства у сфері кримінального та кримінального процесу. Ці зобов'язання мають на меті попередження кіберзлочинності за допомогою розробки відповідних стратегій і заходів, спрямованих на зниження ризику вчинення злочинів і нейтралізацію можливих шкідливих наслідків для приватних осіб і суспільства [13, с.171]. У сучасному світі до таких заходів відносять прийняття більш вдосконалених законів протидії, розвиток потенціалу органів кримінального правосуддя і правоохоронних органів, постійний моніторинг і обмін новітньою інформацією про криміногенну ситуацію, пов'язану із кіберзлочинами.

Система електронно-комп'ютерних порушень, визначена відповідно до законодавства України, охоплює кримінальні дії у таких сферах:

1. Використання електронно-комп'ютерних систем, комп'ютерів і мереж електрозв'язку, у тому числі платіжних систем, включаючи підготовку, вчинення або приховування таких дій.

2. Розповсюдження інформації незаконного характеру з використанням електронно-комп'ютерних систем, комп'ютерів і мереж електрозв'язку.

3. Порушення господарських відносин та приватної власності, включаючи нелегальні фінансові операції та заборонені види господарської діяльності, які реалізуються через мережі електрозв'язку або комп'ютерні системи [8, с.248].

Кіберзлочинність – новий вигляд злочинності, часто має транснаціональний характер. Це сукупність суспільно небезпечних дій, які перебувають під кримінальною відповідальністю держав, включаючи втручання в операції комп'ютерів, модифікацію несанкціонованих даних, а також інші порушення, вчинені через використання комп'ютерів, мереж і програм [30].

Кіберзлочинність розглядається у віртуальному просторі, як зазначають різні дослідники в своїх трактуваннях. Відповідно до думки М.В.Гребенюк, це представляє злочинність у модельованому комп'ютером інформаційному просторі з використанням електронно-обчислювальних машин, телекомунікаційних систем і комп'ютерних мереж [17, с.204].

О.С. Луньова з криміналістичного погляду, визначає кіберзлочин як суспільно небезпечний вторгнення у кіберпростір, що становить загрозу громадській безпеці, власності, правам людини та іншим правовідносинам, захищеним законом. Це також важливий компонент механізму приховування та виконання злочину, а його виявленням є комп'ютерна інформація, яка виступає об'єктом або інструментом правопорушення. Таким чином, питання визначення кіберзлочинності залишається актуальним у сучасній правовій доктрині [48, с.107].

Кіберзлочинність можна розглядати, як:

1. сукупність порушень, спрямованих на комп'ютерні системи та мережі.

2. сукупність незаконних дій, спрямованих на різні типи інформації, з використанням інформаційно-комунікаційних технологій.

3. суспільно-небезпечні дії, які мають місце в кіберпросторі [62, с.146].

У визначенні кіберзлочинності вчені досягли більшої однозначності, концентруючись на характерних особливостях цього явища. Однією з основних характеристик високотехнологічної злочинності є інтелектуальний аспект кіберзлочинності, який вимагає додаткових фахових знань для вчинення протиправних дій. Також важливими рисами є анонімність і

персоналізація, що дозволяє приховати особистість. До інших важливих аспектів відносяться вартість, оскільки і вчинення кіберзлочинів, і їхнє розслідування є високозатратними, а також дистанційність, де місцезнаходження злочинців, місце вчинення злочину та його соціально небезпечні наслідки можуть бути значно віддаленими одне від одного.

Кіберзлочини відрізняються автоматизованістю, оскільки вони можуть призводити до надмірної кількості протизаконних короткотермінових дій, які вчиняються з використанням комп'ютерних технологій. Також вони характеризуються опосередкованістю, де взаємодії між злочинцем і об'єктом злочину, а також між злочинцем і потерпілим, можуть перетворюватися з прямих у опосередковані, наприклад, через електронні пристрої та мережі [67].

Ще однією особливістю є віртуалізація, коли кіберзлочини вчиняються у специфічному кіберпросторі, де протиправна діяльність та її наслідки часто є формально нематеріалізованими. Також слід зазначити транснаціональність або міжнародність, оскільки злочинні дії можуть бути пов'язані з більш ніж однією юрисдикцією або відбуватися на території інших країн. Організованість кіберзлочинності проявляється у формі організованої діяльності, що використовує чорні ринки кіберзлочинності та охоплює різні етапи створення шкідливих програм, управління бот-мережами, а також збір та продаж особистих і фінансових даних [24, с.167].

Необхідно відзначити, що, згідно з Конвенцією ООН проти транснаціональної організованої злочинності, транснаціональними злочинами будуть вважатись ті, що:

a) вчинені в межах територій кількох держав;

b) вчинені тільки в межах території однієї держави, але основна підготовка і вся організація в іншій державі;

c) вчинені в межах території однієї держави, але при взаємодії організованої злочинної групи, яка свою діяльність розповсюджує на кілька держав;

d) скоєні в одній державі, але мають суттєві наслідки в іншій державі [40].

З огляду на особливості кіберзлочинності, внутрішньодержавні норми, що регулюють боротьбу з цим видом злочинності, повинні ґрунтуватися на спеціальних міжнародних стандартах. Ефективний протидія кіберзлочинам стає можливим лише завдяки міжнародному співробітництву. Зважаючи на відсутність узгодженого та визнаного на міжнародному рівні понятійно-категоріального апарату, національні закони можуть містити норми, які не можна ефективно застосувати на практиці. Тому надзвичайно важливим і актуальним завданням міжнародного права є розроблення єдиної міжнародно-правової концепції кіберзлочинності [44, с.39].

Однак важко не погодитися з А.І. Марущак в питанні про необхідність значних змін у криміналізації дій в міжнародно-правовому полі, оскільки вона не відповідає сучасним реаліям. Це особливо стосується області новітніх технологій. Нормативне регулювання, передусім на міжнародному рівні, повинно оперативно адаптуватися до вимог сучасності. Серед таких викликів слід виділити появу нових асиметричних джерел сили, до яких відносяться і кібернетичні [50].

Генеральна Асамблея ООН в своїх рішеннях визначає загрозу використання новітніх технологій, яке порушує принципи міжнародного права та Статут ООН. Особливу увагу приділяється необхідності запобігання використанню інформаційно-комунікаційних технологій у злочинних чи терористичних цілях. Положення Женевської Декларації принципів «Побудова інформаційного суспільства: глобальне завдання в новому тисячолітті» також визначає необхідність створення глобальної культури кібербезпеки у співпраці з усіма зацікавленими сторонами та компетентними міжнародними органами. Глобальна культура кібербезпеки повинна включати в себе захист даних та недоторканість приватного життя [65, с.57].

У зв'язку з цим, ООН разом із міжнародним співтовариством повинна сприяти координованій боротьбі проти використання інформаційно-

комунікаційних технологій в протиправних цілях та забезпечити захист прав людини. Боротьба з кіберзлочинністю визначається як важлива складова глобальної культури кібербезпеки за різними міжнародними документами, але термін сам по собі не має чіткого визначення.

Аналізуючи вищезазначене, можна визначити два підходи до розуміння та трактування кіберзлочинності. У вузькому розумінні, цей термін обмежується конкретним переліком дій, спрямованих на порушення конфіденційності, цілісності та доступності комп'ютерних даних чи систем. У широкому розумінні, він включає різноманітні дії, які можуть бути здійснені з метою особистого або фінансового збагачення, завдання шкоди за допомогою комп'ютера, а також використання особистих і інших даних, що зберігаються в комп'ютері.

Міжнародна система співпраці у сфері боротьби з кіберзлочинністю базується на угодах, укладених в рамках різних регіональних організацій. Зокрема, у Конвенції Ради Європи про кіберзлочинність 2001 року (Конвенція РЄ) зустрічається термін «кіберзлочинність», але сам документ не надає його чіткого визначення [1, с.65]. У конвенції вказано лише конкретні види незаконних дій, які підлягають криміналізації. У вступі до Конвенції РЄ зазначено, що цей документ спрямований на припинення актів, які порушують конфіденційність, цілісність та доступність комп'ютерних систем, мереж і даних, а також зловживання ними. Конвенція призначена для доповнення існуючих угод з метою підвищення ефективності кримінальних розслідувань і переслідувань, пов'язаних із злочинами, пов'язаними з комп'ютерними системами і даними, та для надання можливостей збирання електронних доказів кримінальних злочинів.

Термін «кіберзлочин» використовується в різних міжнародних конвенціях і угодах для опису кримінальних діянь в цифровій сфері. У Конвенції Ради Європи він розглядається як цифровий злочин, спрямований на порушення конфіденційності, цілісності та доступності комп'ютерних систем, мереж і даних. У Конвенції Ліги арабських держав (ЛАД) та Угоді

Співдружності Незалежних Держав (СНД) використовуються терміни «злочини у сфері інформаційних технологій» і «злочин у сфері комп'ютерної інформації» відповідно, проте конкретне визначення цих термінів може відрізнятися в кожному документі [80, с.126].

Зокрема, Конвенція ЛАД має за мету боротьбу із злочинами, пов'язаними з використанням засобів для обробки даних, тоді як Угода СНД спрямована на кримінальне покарання дій, що зачіпають комп'ютерну інформацію [75]. Відмінності в термінології можуть впливати на обсяг і види злочинів, що підпадають під їхні покарання та регулювання.

Такий підхід до визначення кіберзлочинів у міжнародних документах відзначається спробою врахувати різноманітні аспекти цифрової безпеки та небезпек, які можуть виникнути внаслідок зловживань інформаційно-комунікаційними технологіями.

Угода про співробітництво у сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва 2009 року включає термін «інформаційна злочинність», що визначається як використання інформаційних ресурсів та/або вплив на них в інформаційному просторі у протиправних цілях [74]. Конвенція про кібербезпеку і захист персональних даних Африканського Союзу 2014 року використовує термін «кіберзлочинність» (cybercrime, cyber-crime).

В ході аналізу статті 25 «Законодавство проти кіберзлочинності» визначається, що кожна Держава-Учасниця повинна приймати заходи для боротьби з кіберзлочинністю, охоплюючи кримінальні злочини, що впливають на конфіденційність, цілісність, доступність та збереження ІКТ, а також ефективні процедурні заходи [68, с.97].

Отже, виходячи з аналізу положень цих міжнародних договорів, можна припустити, що поняття «кіберзлочинність», «злочини у сфері інформаційних технологій», «злочини у сфері комп’ютерної інформації» та «інформаційна злочинність» визначають схожі аспекти злочинів у цифровому просторі. Однак, для повноти відповіді, необхідно провести

детальний аналіз сфери застосування кожного з цих термінів в міжнародному контексті.

На практиці, кожен із укладених договорів про кіберзлочинність націлений на протидію конкретним видам протиправних дій, переліки яких не є ідентичними один одному. Важливо зауважити, що криміналізація дій, пов'язаних із кіберзлочинністю, є окремою науковою та практичною проблемою, яка буде розглянута більш детально у наступному параграфі.

Таким чином, можна визнати, що за сферою дії Конвенції РЄ, ЛАД, АС, Угоди СНД і Угоди ШОС поняття «кіберзлочин», «злочин у сфері інформаційних технологій», «злочини у сфері комп'ютерної інформації» та «інформаційна злочинність» не можна вважати тотожними. З іншого боку, ці терміни об'єднуються загальними рисами:

- є видами кримінально караних дій, іншими словами, злочинами;
- здійснюються в електронному / віртуальному середовищі;
- включають в себе зв'язок правопорушення з комп'ютерними системами, мережами, даними, ІКТ / засобами зберігання, сортуванням, отриманням, обробкою, розробкою та обміном інформацією / комп'ютерною інформацією / інформаційними ресурсами та інформаційним простором.

Важливою у контексті обговорюваного питання є офіційне тлумачення положення статті 1.a. Будапештської конвенції, надане Комітетом з Конвенції про кіберзлочинність Ради Європи. Згідно з цим тлумаченням від 2012 року, комп'ютерні системи включають різноманітні пристрої, наприклад, мобільні телефони, які виконують різні функції та можуть обробляти, створювати та передавати дані (наприклад, доступ до Інтернету, відправлення повідомлень, завантаження контенту тощо) [76, с.184].

Під час виконання своїх завдань різноманітні гаджети проводять обробку «комп'ютерних даних» (згідно зі статтею 1.b. Будапештської конвенції) та створюють «дані про рух інформації» (згідно зі статтею 1.d. Будапештської конвенції). Таким чином, визначення «комп'ютерна система»

охоплює різноманітні форми комп'ютерних технологій, що виходять за рамки традиційного їх розуміння, такі як смартфони, планшети, кишенькові персональні комп'ютери та інші.

У процесі формування термінологічної бази в сфері протидії кіберзлочинності важливе значення мають рішення міжнародних міжурядових організацій та інші джерела «soft law». Зокрема, до цих джерел відносяться Висновки Організації економічного співробітництва та розвитку «Злочини, пов'язані з комп'ютером: аналіз правової політики» (1985 р.), Рекомендація № R89 (9) Комітету міністрів держав – членів Ради Європи про злочини, які пов’язані з комп’ютерами (1989 р.), Рекомендація, прийнята на VIII Конгресі ООН з попередження злочинності та поводження з правопорушниками (1990 р.), Рекомендація про керівні принципи забезпечення безпеки інформаційних систем (1992 р.), Довідник ООН із запобігання і контролю злочинності, пов’язаної з комп’ютерами (1995 р.), Десять принципів боротьби з високотехнологічними злочинами, прийняті на зустрічі міністрів внутрішніх справ та міністрів юстиції Великої Вісімки (1997 р.), План дій про боротьбу із злочинами, пов’язаними з використанням високих технологій та комп’ютерів Комісії з попередження злочинності та кримінального правосуддя (2001 р.) та інші [6, с.34].

Крім терміна «кіберзлочинність», у вказаних актах використовуються такі поняття, як «злочини пов’язані з комп’ютерами», «злочини, пов’язані з використанням комп’ютерних технологій» і «високотехнологічні злочини» [6, с.35]. Джерела soft law мають рекомендаційний характер і не є обов'язковими. Однак, на нашу думку, врахування їх при формуванні універсальної концепції кіберзлочинності було б доцільним.

Таким чином, як у науці, так і в практиці міжнародного права відсутня єдність та однозначність визначення і застосування поняття «кіберзлочинність». Це значуще складається на зменшення ефективності правового регулювання в цій сфері та спричинює виникнення прогалин і

колізій. Одночасно стрімкий технологічний прогрес свідчить про те, що ця проблема в майбутньому буде тільки загострюватися.

РОЗДІЛ 2
ПРАВОВЕ РЕГУЛЮВАННЯ БОРОТЬБИ ТА СПІВРОБІТНИЦТВА В ПИТАННЯХ КІБЕРЗЛОЧИННОСТІ

2.1. Нормативно-правове регулювання боротьби з кіберзлочинністю на міжнародному рівні

До сфери проблем, які викликають загальну тривогу у світовій спільноті, відноситься транснаціональна злочинність. Це новий рівень організованої злочинності, який перетинає кордони та ігнорує національні та міжнародні закони і норми. Спрямованість держав на протидію транснаціональній організованій злочинності реалізується у боротьбі з різними її проявами, такими як незаконний обіг наркотиків, терористичні акції, «відмивання» грошей, незаконне ввезення мігрантів, торгівля людьми, незаконний обіг вогнепальної зброї, фальшування грошей та кіберзлочини.

Міжнародне кримінальне право розробило механізми і стратегії для боротьби з транснаціональною злочинністю, і важливе місце серед них відводиться міжнародно-правовому регулюванню протидії кіберзлочинності. Цей вид злочинів може стрімко зростати, а методи його вчинення розвиваються нерізноманітно, часто випереджаючи заходи захисту комп'ютерної інформації.

Одним із базових документів для європейських країн у боротьбі з кіберзлочинністю є Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. [42] та її Додатковий протокол від 28.01.2003 р. [31]. Ці документи є основою для розробки відповідного законодавства європейських країн та відзначаються тим, що навіть держави, які не є членами Ради Європи, такі як Канада, Ізраїль, Південна Африка, США, підписали та ратифікували їх. Конвенція про кіберзлочинність не надає визначення терміну «кіберзлочин», проте надає перелік та класифікацію таких злочинів, що рекомендує встановлювати кримінальну відповідальність національним

рівнем. Такий перелік став основою для визначення терміну «кіберзлочин» у зарубіжній кримінології.

Зокрема, у зазначеному міжнародному документі кіберзлочини поділяються на такі групи:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем (наприклад, незаконний доступ, нелегальне перехоплення);

2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами);

3) правопорушення, пов'язані зі змістом (наприклад, дитяча порнографія, расизм і ксенофобія);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [42].

Використана класифікація кіберзлочинів у Конвенції про кіберзлочинність не є ідеальною, оскільки групи виділяються за різними критеріями. Однак незважаючи на усі недоліки, важливість цього документа беззаперечна, і належна імплементація його положень у національне законодавство держав-підписантів вважається однією з основних рекомендацій, що випливають із дослідження Європолу у 2016 році.

На підставі викладеного можна зазначити, що в зарубіжній кримінології використовується функціональний підхід до визначення кіберзлочину. Вчені зосереджуються не на формулюванні визначення цього поняття, а на визначенні переліку кібердіянь, які вважаються суспільно небезпечними і, відповідно, повинні бути криміналізовані.

Такий підхід також використовується у Конвенції про кіберзлочинність, де акцент робиться не на роз'ясненні змісту понять «кіберзлочин» та «кіберзлочинність», а на визначенні їх обсягу – конкретних дій, які відносяться до кіберзлочинів і, відповідно, формують концепцію кіберзлочинності.

З урахуванням міжнародного характеру положень Конвенції про кіберзлочинність [42] такий підхід є виправданим і обумовлений необхідністю ефективної реакції правоохоронних органів на національному та міжнародному рівнях на зростаючу кількість кіберзлочинів, а також сприяє налагодженню співпраці у розслідуванні цих злочинів та притяганню винних до кримінальної відповідальності.

Безперечно, для ефективного міжнародного співробітництва необхідно встановити єдиний підхід стосовно кваліфікації міжнародно-правових явищ. У даному випадку маємо на увазі вчинення злочину, що визначається не лише наявністю незаконної поведінки особи, але й її кваліфікацією як забороненої сторонами співробітництва.

У міжнародному кримінальному праві цей принцип закріплений у формі «подвійної кримінальності». Згідно з цим принципом, держава-потерпіла та держава, яку звертаються із запитом про співробітництво, можуть незалежно притягнути особу до відповідальності за вчинену дію. Іншими словами, дії можуть бути кваліфіковані та карані обома державами паралельно. Такий підхід передбачає ідентичність злочину для обох сторін, що характеризується однаковою суспільною небезпекою та відповідністю санкцій згідно з національним законодавством тощо [52, с.18].

Конвенція встановлює новий міжнародний стандарт для «кіберзлочину». Це агреговане поняття, яке охоплює кілька видів протиправної поведінки, таких як атаки на комп'ютерні дані і системи, незаконне використання роботи комп'ютерів, а також дії, пов'язані з розповсюдженням забороненої чи використанням інформації, що підпадає під правовий захист.

Організація Об'єднаних Націй, Рада Європи, Європейський Союз, Організація з безпеки і співробітництва в Європі та інші впливові міжнародні організації активно займаються розробкою концепції протидії кіберзлочинності та формулюванням узгодженої політики стримування цієї

загрози. Ця ініціатива включає проведення міжнародних конгресів та форумів, прийняття конвенцій та резолюцій тощо.

Особлива увага була приділена проблемі злочинності, пов'язаної з використанням комп'ютерів, на Одинадцятому конгресі ООН з попередження злочинності і кримінального правосуддя (Бангкок, Таїланд, квітень 2005 р.). Відзначено, що кіберзлочинність має унікальний характер, і для ефективного протидії їй необхідно застосовувати комплексні стратегії. Експерти ООН рекомендують вжити невідкладних заходів щодо оновлення кримінального законодавства держав-учасниць, зокрема, уточнення або вилучення застарілих норм і введення нових положень, що відповідають сучасним викликам у сфері кіберзлочинності [64, с.387].

На Конгресі відзначалося, що поширення нових інформаційно-комунікаційних технологій по всьому світу призвело до збільшення числа різноманітних злочинів, пов'язаних з використанням комп'ютерів. Ці злочини не лише становлять загрозу конфіденційності, цілісності та доступності комп'ютерних систем, а й підіймають питання безпеки важливих елементів інфраструктури. Технологічні новації породжують різноманітні тенденції у сфері «кримінальної інновації», що відображає розбіжності, спричинені «розривом у цифрових технологіях».

Глобальна доступність електронних та віртуальних послуг призводить до того, що злочинність в інформаційному просторі має природний транснаціональний характер. Зазначено, що в умовах глобалізації транснаціональної організованої злочинності укладання двосторонніх договорів розглядається як застаріле явище. Організована злочинність допускає незаконну діяльність у кількох державах, які можуть не мати двосторонніх угод про правову допомогу. Нові інструменти міжнародного співробітництва та правової допомоги у кримінальних справах призначені відкривати можливості для співпраці між більшим числом держав [69, с.92].

Бангкокська декларація, яка виникла на Одинадцятому конгресі ООН з попередження злочинності та кримінального правосуддя, підкреслює

актуальність проблеми кіберзлочинності. Стримування кіберзлочинності є необхідною складовою частиною національної кібербезпеки та стратегії захисту важливої інформаційної інфраструктури. Є.Д. Скулиш наголошує, що національна відповідальність вимагає спільних дій з боку урядових організацій, приватного сектора і громадян, а на регіональному і міжнародному рівнях вона передбачає кооперацію та координацію зусиль держав [69, с.92].

С.В. Демедюк вказує на те, що сучасне інформаційне середовище сприяє зростанню злочинності, а «інформація – злочинність» взаємодіє системно і стійко. Розвиток інформаційного мегасередовища призводить до глобалізації злочинності, що швидко розширюється. Незважаючи на зовнішню різноманітність цих явищ, спостерігається тісний зв'язок і тенденція до його посилення [20, с.67].

На сьогоднішній день відсутні адекватні статистичні дані, які відобразили б реальну картину стану кіберзлочинності, і немає надійних методів їх збору. Крім того, відсутня єдина національна кримінальна законодавча база держав у сфері протидії кіберзлочинності. Поняття «комп'ютерний злочин» чи «злочин, пов'язаний з використанням комп'ютерів» обговорюються протягом останніх 50 років, проте до цього часу вони не мають однозначного визначення.

У нормативних правових актах терміни «кіберзлочинність», «комп'ютерні злочини», «злочини, з використанням електронних засобів зв'язку», «злочини у сфері високих технологій», «ІТ-злочини» часто взаємозамінюються. У контексті нашого дослідження кіберзлочинність визначається як злочинність, що виникає у кіберпросторі.

Міжурядова група експертів, створена Комісією з попередження злочинності і кримінального правосуддя ООН, відзначила що «комп'ютерна злочинність і, зокрема, кіберзлочинність» – це терміни, які використовуються для опису конкретної категорії злочинів. Проблеми, пов'язані з цією

категорією, включають не лише широкий спектр вже відомих порушень, а й нові методи вчинення злочинів, що стрімко розвиваються.

У матеріалах ООН терміни «кіберзлочини» описують будь-який протиправний акт, який може бути здійснений за допомогою комп'ютерної системи чи мережі, всередині або проти них. Таким чином, до кіберзлочинів можна віднести будь-який злочин, який відбувається в електронному середовищі [34, с.3]. Комп’ютерні злочини, за словами О.О.Йона, включають в себе розповсюдження шкідливих вірусів, взлом паролів, крадіжку номерів кредитних карт, поширення протиправної інформації – від брехні до матеріалів порнографічного характеру [35].

На початку XXI століття з'явилися нові комп’ютерні злочини, такі як фішинг, атаки з використанням бот-мереж, IP-телефонія і інші. О.М. Косогов розробила класифікацію кіберзлочинів, в яку входять:

1) Насильницькі або інші потенційно небезпечні кіберзлочини, що ставлять під загрозу фізичну безпеку, життя та здоров'я людини;

2) Злочини, які порушують конфіденційність інформації, такі як незаконний доступ до комп'ютерів чи комп'ютерних систем без завдання шкоди інформації;

3) Деструктивні кіберзлочини, які включають пошкодження даних і порушення цілісності даних і безпеки функціонування комп'ютерних систем;

4) Злочини, які зачіпають майно, майнові права, а також право власності на інформацію і авторські права;

5) Злочини, які порушують суспільну мораль;

6) Інші кіберзлочини, такі як «computer-facilitated» (традиційні злочини, вчинення яких полегшує або відкриває нові можливості комп'ютер) [43, с.147].

Для більшості злочинів, які відбуваються у глобальних комп’ютерних мережах, характерні наступні особливості:

– високий ступінь таємниці під час вчинення злочину, що обумовлено специфікою інформаційного простору мережі (застосування вдосконалених механізмів анонімності, складність інфраструктури тощо);

– транснаціональний характер мережевих злочинів, де злочинець, об'єкт злочинного посягання та потерпілий можуть перебувати на територіях різних держав;

– особливий рівень підготовки злочинців, інтелектуальний характер злочинної діяльності;

– нестандартність, складність, різноманітність і часте оновлення методів та засобів для вчинення злочинів;

– можливість автоматизованого вчинення злочину в кількох місцях одночасно;

– багатоепізодний характер злочинних дій у випадку численних потерпілих;

– неосвіченість потерпілих щодо того, що вони стали жертвами злочинного втручання;

– дистанційний характер злочинних дій в умовах відсутності фізичного контакту між злочинцем та потерпілим;

– неможливість попередження та припинення цього виду злочину традиційними засобами [72, с.76].

Необхідність розвитку міжнародного співробітництва в інформаційному просторі з метою запобігання кіберзлочинам підтверджується наступними міжнародними документами: Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті», що була прийнята 12 грудня 2003 року представниками народів світу, що зібралися у Женеві для проведення першого етапу Всесвітньої зустрічі на вищому рівні по питанням інформаційного суспільства; «Окінавська Хартія глобального інформаційного суспільства», прийнята 22 липня 2000 року лідерами країн «Великої вісімки», Туніська

програма для інформаційного суспільства, прийнята у 2005 році, та Програма «Інформація для всіх», яка була прийнята в 2001 році ЮНЕСКО [82, с,395].

Міжнародні нормативно-правові акти універсального та регіонального характеру становлять правову основу для протидії кіберзлочинам. Зокрема, Конвенція ООН проти транснаціональної організованої злочинності від 15 листопада 2000 року [40] відображає основні напрямки міждержавного співробітництва в цій сфері. Оскільки кіберзлочини мають транснаціональний характер і можуть завдавати значної шкоди економічному розвитку держав, міжнародна спільнота докладає зусиль для мінімізації їх впливу на міжнародні економічні відносини.

На конференції з економічних злочинів у 1976 році Рада Європи також підкреслила транснаціональний характер комп'ютерних злочинів. Основні риси транснаціональності та транснаціонального характеру злочинів наведено в статті 3, пункті 2 Конвенції 2000 року. Згідно з цим документом, злочин вважається транснаціональним, якщо він вчинений у більш ніж одній державі, або якщо в одній державі вчинений злочин, але істотна частина його підготовки, планування, керівництва чи контролю відбувається в іншій державі. Також транснаціональний злочин може бути вчинений в одній державі за участю організованої злочинної групи, яка здійснює злочинну діяльність у більш ніж одній державі, або якщо його істотні наслідки відбуваються в іншій державі [9, с.41].

Серед регіональних правових інструментів слід визначити Конвенцію про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу, яка була прийнята 29 травня 2000 року [41], зокрема в розділі III «Перехоплення телекомунікаційних повідомлень». Однак базовими документами для протидії кіберзлочинності є Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року та її Додатковий протокол від 28 січня 2003 року. Ці документи становлять «основу для розробки відповідного законодавства європейських держав» [1, с.68].

Розробка Конвенції про кіберзлочинність Радою Європи розпочалася під час конференції з економічних злочинів у 1976 році. Створений на цій конференції Комітет експертів з питань злочинності у кіберпросторі підготував 25 проєктів тексту конвенції. Остаточний текст був схвалений на засіданні Комітету Міністрів в ранзі постійних представників 19 вересня 2001 року та прийнятий міністрами іноземних справ 8 листопада 2001 року. 23 листопада 2001 року в Будапешті Конвенція Ради Європи про кіберзлочинність була відкрита для підписання та набула чинності 1 липня 2004 року [1, с.66].

У 2003 році був схвалений Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації дій расистського і ксенофобського характеру, здійснюваних за допомогою комп'ютерних систем [1]. Згідно з Конвенцією 2001 року, держави-учасниці зобов'язані гармонізувати національні закони щодо визначення основних злочинів. Кожна сторона повинна приймати заходи, необхідні для кваліфікації широкого спектру дій як кримінальних злочинів відповідно до свого внутрішньодержавного права. Конвенція розрізняє два види протиправних дій, пов’язаних з кіберзлочинністю: злочини та правопорушення.

Частина I Другого розділу Конвенції («Матеріальне кримінальне право») поділяє всі склади злочинів на підрозділи (групи) за родовим об’єктом, якими здійснюється посягання. У Конвенції виділено чотири види комп’ютерних злочинів:

1) злочини проти конфіденційності, цілісності і доступності комп’ютерних даних і систем;

2) правопорушення, пов’язані з використанням комп’ютерних засобів;

3) правопорушення, пов’язані із змістом даних;

4) правопорушення, пов’язані з порушенням авторського права і сумісних прав. Крім того, визначені додаткові види відповідальності і санкцій, такі як замах та співучасть.

Протокол до Конвенції про кіберзлочинність 2003 року розширює коло злочинів та включає зобов'язання щодо криміналізації ряду дій. Серед них:

1. Поширення расистських і ксенофобських матеріалів через комп'ютерні системи (ст. 3).

2. Мотивована загроза расизму і ксенофобії через комп'ютерну систему здійснення серйозного кримінального злочину щодо осіб, що належать до різних груп (ст. 4).

3. Публічна расистська і ксенофобська образа через комп'ютерну систему (ст. 5).

4. Поширення чи надання доступу для громадськості через комп'ютерну систему матеріалу, який заперечує чи применшує негативні наслідки, схвалює чи виправдовує дії, що є геноцидом чи злочинами проти людяності, як визначено міжнародним правом та підтверджено рішеннями міжнародних судів (ст. 6) [1, с.67].

Норми Конвенції Ради Європи про кіберзлочинність 2001 року активно використовуються та мають відображення у національних законодавствах. Деякі положення можуть бути спірними, зокрема, норма ст. 32 пункт b, що дозволяє будь-якій Стороні здійснювати доступ до комп'ютерних даних на території іншої Сторони за наявності законної і добровільної згоди особи з відповідними повноваженнями [1, с.68].

Цей пункт уповільнює співробітництво між державами та ефективне вирішення різноманітних питань у сфері кібербезпеки і водночас порушує право на приватне життя, яке є одним із ключових принципів міжнародного права. Також існують труднощі при підписанні та впровадженні норм у національне законодавство, чого свідчить той факт, що за 20 років з моменту укладання Конвенції ратифікували її лише 47 держав, із яких 37 є членами Ради Європи. Крім того, міжнародний характер Конвенції, який передбачає відкритість для приєднання всіх зацікавлених держав, включає ряд обмежень, таких як процедура приєднання країн, що не є членами Ради Європи, яка

вимагає консультацій та одноголосного рішення держав-членів Ради Європи [14].

Держави, що підписали цю Конвенцію, зобов'язані впроваджувати політику протидії кіберзлочинності на міжнародному рівні, сприяти цій протидії та розслідувати злочини, скоєні в глобальній інформаційно-цифровій мережі, а також брати участь у формуванні нових заходів протидії кіберзлочинності.

Основні проблеми, що виникають при міжнародно-правовому регулюванні протидії кіберзлочинності, включають різницю у національних законах щодо кібербезпеки, відсутність єдиної системи категоризації, недостатню координацію правоохоронних органів при розслідуванні кіберзлочинів, обмежений обмін інформацією про кіберінциденти між країнами та недостатню взаємодію між секторами державного та приватного секторів у цій області.

Як зазначає О.О.Грицун, потреба у міжнародно-правових стандартах виникає для стимулювання встановлення кримінально-правової заборони та гармонізації національного законодавства [19, с.173]. Велика частина внутрішньодержавного права країн має значний ступінь подібності щодо більшості традиційних видів транснаціональних злочинів, проте нові форми злочинності потребують узгоджених визначень. У справі боротьби з кіберзлочинністю, проблема гармонізації кримінально-правової заборони набуває особливого значення.

Однією з ключових особливостей кіберзлочинності є її глобальний та інтернаціональний характер, що ускладнює ефективність традиційних методів протидії. Для успішної боротьби з цим явищем держави повинні співпрацювати, хоча така взаємодія в певній мірі може зачіпати державний суверенітет та повноваження у сфері захисту інформації. Найбільш ефективна міжнародна співпраця в цьому напрямку можлива в рамках високого рівня політичної довіри, як у Європейському Союзі.

Міжнародна діяльність щодо протидії кіберзлочинності визначається роботою Міжнародного центру протидії кіберзлочинності, створеного у 2013 році у Гаазі. Цей центр зосереджений на розробці нових методів розслідування кіберзлочинів.

Організація Об'єднаних Націй та її спеціалізовані установи, зокрема Управління ООН з наркотиків та злочинності, відіграють ключову роль у цьому процесі (UNODC). Це управління виконує важливі функції, зокрема через Глобальну програму з кіберзлочинності та Міжурядову експертну групу відкритого складу з кіберзлочинності. Ці установи сприяють збільшенню потенціалу боротьби з кіберзлочинністю, надаючи підтримку національним структурам і заходам [19, с.175].

В Європейському Союзі існують нормативно-правові акти, спрямовані на протидію протиправним посяганням на електронні інформаційні ресурси. Серед них Директива ЄС щодо протидії кібератакам на інформаційні системи, прийнята у 2013 році, та Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет, прийнята у 2017 році. У рамках ЄС велика увага приділяється питанням раннього виявлення та оперативного реагування на кіберінциденти та кібератаки, спрямованих проти електронних інформаційних ресурсів [22, с.111].

Наприклад, в Стратегії кібербезпеки Європейського Союзу, під поняттям «кіберзахист» включається виявлення і блокування кібератак, локалізація їх наслідків незалежно від походження стосовно цивільних об’єктів усіх форм власності, а також встановлення і розслідування кіберзлочинів. Європейська агенція мережевої та інформаційної безпеки (ENISA) виконує функції виявлення і блокування кібератак, а також локалізації їх наслідків [22, с.112].

Прикладами успішної співпраці, ґрунтованої на правовій взаємодії кількох держав, можна вказати випадки, коли вони, шляхом укладання регіональних угод, досягли високого рівня гармонізації своїх правових норм і розвинули ефективні механізми взаємодії, враховуючи особливості

кіберзлочинів. В цьому контексті матеріальне право визначено через ряд директив, таких як Директива про протидію сексуальній експлуатації дітей онлайн і дитячої порнографії, а також Директива про безпеку мереж та інформаційних систем.

Спостереження за негативними явищами в кіберпросторі, включаючи протизаконні дії, вимагає активізації міжнародного партнерства у порівнянні з заходами, спрямованими проти інших форм міжнародної злочинності. Зокрема, на додаток до гармонізації кримінально-правових норм, важливо забезпечити гармонізацію процедурних механізмів і розгортання нових аспектів міжнародного партнерства.

Значущий внесок у протистоянні кіберзлочинності мають міжнародні договори в цій сфері, такі як: Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 року, Модельний Закон країн Карибського басейну про кіберзлочинність, спільний проєкт Європейського Союзу і Міжнародного Союзу Електрозв'язку для країн Тихоокеанського регіону, проєкт ООН з розробки законодавства в галузі кіберзлочинності для країн Африки та інші [22, с.114].

Розуміння необхідності розробки та прийняття міжнародно-правових актів для протидії комп'ютерним злочинам стало широко прийнятим серед міжнародних організацій, що належать до 1990-х років. Організація Об'єднаних Націй (ООН), враховуючи важливість інформації, розвиток інформаційно-комунікаційних технологій, створення світових баз даних, глобальних інформаційних мереж і систем та їх захисту, прийняла координуючу роль у розробці концептуальних та правових засад регулювання ключових аспектів. Серед них – боротьба з злочинним використанням інформаційних технологій, яка визначена в резолюціях Генеральної Асамблеї ООН з 2011 по 2016 рік [73, с.80].

Крім того, Економічна і Соціальна Рада ООН прийняла резолюції, спрямовані на захист особистих даних (резолюції ЕКОСОР «Міжнародне

співробітництво у справі попередження і розслідування шахрайства, злочинного неправомірного використання і фальсифікації особистих даних і пов'язаних з ними злочинів, а також переслідування та покарання за них» [73, с. 80]. Резолюцією Генеральної Асамблеї A/RES/58/199 особливо акцентовано на потребі захисту інформаційних інфраструктур, зазначаючи важливі компоненти для їх ефективного захисту.

Маючи на увазі формування сприятливих умов для прогресу інформаційно-комунікаційних технологій, Організація Об'єднаних Націй співпрацює з Комісією Африканського Союзу в рамках програми «Нове партнерство на користь розвитку Африки» для розробки конвенції з кібербезпеки в Африці на зразок Конвенції про кіберзлочинність.

Світові розбіжності у сфері положень про співпрацю, які містяться в різних багатосторонніх чи двосторонніх документах, відсутність зобов'язання надавати відповіді протягом визначеного терміну, відсутність узгодженості щодо припустимого прямого доступу до екстериторіальних даних, наявність багатьох неформальних мереж правоохоронних органів та відмінностей у гарантіях співпраці – усе це представляє серйозні труднощі у забезпеченні ефективної міжнародної співпраці в галузі електронних доказів у кримінальних справах [68, с.97].

У контексті дослідження питань міжнародно-правового регулювання інформаційного тероризму слід зазначити проєкт «Загального договору з питань кібербезпеки та кіберзлочинності», який був запропонований професором Штайном Шольбергом, головою групи експертів високого рівня з кібербезпеки, заснованою у 2007 році для вивчення можливостей створення загального документа з питань кіберзлочинності в Організації Об'єднаних Націй, а також професором Соланж Гернуті-Елі.

Автори цього проєкту розглядають інформаційний тероризм як один із видів кібератак, включаючи публічне підбурювання до вчинення терористичного злочину, набір і схилення людей для вчинення терористичних актів та проведення терористичних навчань. Проєкт також

передбачає кримінальну відповідальність за ці дії згідно з внутрішнім законодавством держав-учасниць. В межах ЮНЕСКО була розроблена концепція «Універсальності Інтернету», яка відображає позицію організації стосовно питань, пов'язаних з Інтернетом, на період до 2021 року [81, с.302].

Відзначаючи роль Інтернету у розвитку суспільств знань та досягненні цілей сталого розвитку ООН, концепція «Універсальності Інтернету» має чотири ключові принципи, відомі як принципи R.O.A.M. – орієнтованість на права людини, відкритість, доступність та багатостороння участь. В цьому контексті виникає концепція Конвенції ООН про забезпечення міжнародної інформаційної безпеки, яка ідентифікує основні загрози міжнародному миру та безпеці в інформаційному просторі, визначаючи 11 базових та 4 додаткових загрози, включаючи використання інформаційних технологій для ворожих дій, деструктивний вплив на критично важливі структури та транскордонне поширення інформації, що суперечить принципам міжнародного права.

З метою оптимізації надання взаємної правової допомоги в справах електронних доказів, Управління Організації Об'єднаних Націй з наркотиків і злочинності впроваджує нововведення, такі як включення модуля по електронним доказам в перероблену Програму складання прохань про надання взаємної правової допомоги. За одночасного впровадження цих ініціатив, правоохоронні органи починають відчувати зростаючу потребу в розробці новаторських методів співпраці в сфері транснаціональних розслідувань кіберзлочинів [83].

Особливу важливість може мати участь в координації підтримки транснаціональних розслідувань з боку структур, таких як Глобальний інноваційний комплекс Інтерполу та Європейський центр по боротьбі з кіберзлочинністю Європолу. Інші ініціативи, такі як Глобальна конференція з кіберпростору, також відкривають можливості для розгляду інноваційних заходів у сфері міжнародного співробітництва в протидії кіберзлочинності.

Світова організація інтелектуальної власності встановлює нагляд за дотриманням Інтернет-договорів 1996 року, що включають Договір про авторське право та Договір про виконання та фонограми. Ці договори накладають обов'язок на держави-учасниці забезпечувати належний рівень правового захисту та ефективні засоби правового захисту, які запобігають обхід технологічних обмежень, використованих для захисту об'єктів інтелектуальної власності.

На жаль, Всесвітня організація інтелектуальної власності зазнала невдачі у встановленні нормативних положень щодо веб-мовлення та трансляції в Інтернеті, а також у розширенні прав телерадіокомпаній у кіберпросторі.

2.2. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності

Від самого початку 80-х років XX століття у численних країнах виникла усвідомленість того, що національне кримінальне законодавство, ґрунтоване на загальноприйнятих принципах, не забезпечує ефективний захист комп'ютерної інформації. Багато країн прийшли до висновку, що для успішного протистояння комп'ютерній злочинності необхідні узгоджені міжнародні заходи та взаємодія.

На засіданні Генеральної Асамблеї ООН у вересні 1991 року було визнано, що «наростання транснаціональної злочинності становить загрозу внутрішній безпеці країн, свободі людини та міжнародним відносинам, що потребує ефективних міжнародних механізмів та тісної співпраці між країнами» [85, с.1].

Але для створення єдиної міжнародної нормативної бази та нових механізмів потрібен єдиний підхід до розуміння проблеми, формування спільної мети та універсальних принципів. Поточний аналіз закордонного кримінального законодавства свідчить про відсутність єдиного розуміння

того, що вважається комп'ютерними злочинами і яке юридичне визначення має кожен з них.

Різноманітні підходи до визначення та характеристики комп'ютерних злочинів ускладнюють виявлення та покарання злочинців, особливо коли злочин відбувається в одній країні, а його наслідки відчутні в іншій, де такі дії можуть бути об'єктом кримінального переслідування. Неузгоджений підхід ускладнює ефективну боротьбу з комп'ютерною злочинністю.

Отже, система міжнародно-правових механізмів грає визначальну роль у стандартизації національного кримінального законодавства різних країн у контексті комп'ютерної злочинності, пропонуючи спільні та узгоджені концепції. У цьому контексті виділяється ініціатива Організації економічного співробітництва та розвитку, яка в 1983–1985 роках утворила спеціальний комітет для розгляду можливостей гармонізації кримінального законодавства різних країн у справах відповідальності за комп'ютерні злочини [9, с.57].

ОЕСР висунула пропозиції щодо визнання кримінальними наступних дій:

– свідоме втручання у дані чи програми з метою незаконного переведення грошей;

– виготовлення підроблених комп'ютерних даних чи програм з наміром обдурити;

– спричинення шкоди даним чи програмам з метою завадити функціонуванню систем;

– порушення прав на комп'ютерні програми для комерційного використання;

– несанкціонований доступ та захоплення інформації без дозволу особи, відповідальної за систему [9, с.58].

Перший документ, що регулює питання комп'ютерної злочинності в рамках Ради Європи, представлений Рекомендацією № R 89(9) від Комітету Міністрів країн-членів Ради Європи і прийнятий 13 вересня 1989 року. У цьому документі використовується термін «злочин, пов'язаний із

використанням комп'ютерних технологій», і рекомендується внести зміни до національного кримінального законодавства, щоб включити такі дії, як комп'ютерне шахрайство, підроблення, завдання шкоди комп'ютерним даним, комп'ютерний саботаж, несанкціонований доступ, несанкціоноване перехоплення, несанкціоноване відтворення комп'ютерних програм та мікросхем.

Серед категорій злочинів, які можуть викликати дискусії, можна виокремити наступні:

а) Незаконне втручання у комп'ютерні дані чи програми, включаючи недозволені дії у сфері комп'ютерних даних чи програм.

б) Шпигунство у сфері комп'ютерів, що передбачає отримання, розкриття, передачу або використання торговельної чи комерційної таємниці за допомогою неправомірних методів з метою завдання економічних збитків особі, яка має доступ до цієї таємниці, або для отримання незаконної економічної вигоди.

в) Незаконне використання комп'ютера, що означає недозволене використання комп'ютерної системи або мережі, яке може призвести до ризику нанесення шкоди системі чи її функціонуванню, з наміром завдати шкоди особі, яка має право на використання системи.

г) Незаконне використання програми, що охороняється законом, включаючи незаконне використання авторських програм з метою незаконного отримання економічної вигоди або завдання шкоди власнику відповідного права [10, с.24].

Рекомендація № R 89(9) мала за мету встановлення принципу чіткого визначення кримінально-караних дій в рамках положень кримінального закону. Цей принцип визнається як важливий, однак не всі держави його прийняли, і до них відноситься, зокрема, Росія.

Одночасно сама Рекомендація, вказана вище, не надавала чіткого визначення терміну «злочин, пов'язаний з використанням комп'ютерних технологій». Вона оперувала конкретним переліком дій, зазначених у

документі, що давав уявлення про раніше наведені злочини. Цей документ служив орієнтиром для багатьох країн Європи у вдосконаленні кримінального законодавства і сприяв наближенню національного законодавства різних країн. Проте, важливо враховувати його рекомендаційний характер [10, с.26].

Незважаючи на позитивний вплив, не всі європейські держави досягли достатнього зближення у принципових питаннях, що породжує проблеми у систематичній боротьбі з комп'ютерними злочинами. Крім того, у Рекомендації відзначено відсутність кримінально-процесуальних норм. Наступним етапом у розвитку міжнародного співробітництва проти комп'ютерних злочинів стала ініціатива робочої групи Міжнародної організації кримінальної поліції Інтерпол на початку 90-х років. Ця група розробила кодифікатор комп'ютерних злочинів, який пізніше був використаний для створення автоматизованої інформаційно-пошукової системи. Його застосовують для обміну запитань та повідомлень про злочини в галузі комп'ютерних технологій через мережу Міжнародної організації кримінальної поліції Інтерпол.

В галузі комп'ютерної інформації існує широкий спектр злочинних дій, проте не всі з них є кримінальними згідно з національними законами. Протягом 90-х років G-8 провела численні консультації, спрямовані на вирішення проблеми комп'ютерної злочинності.

У липні 2000 року відбулася нарада керівників країн G-8 в Окінаві (Японія), на якій було визнано актуальність «спільного підходу у сфері боротьби зі злочинами в галузі високих технологій, такими як кіберзлочини, які можуть серйозно загрожувати безпеці та довірі в глобальному інформаційному просторі». Цей загальний підхід відобразився в Окінавській Хартії про глобальне інформаційне суспільство, прийнятій на цій нараді, де було зазначено, що «зусилля міжнародного співтовариства у розвитку глобального інформаційного суспільства повинні супроводжуватися

узгодженими діями щодо створення безпечного та вільного від злочинності кіберпростору» [19, с.176].

Додатковий протокол II до Конвенції про кіберзлочинність (Будапештська конвенція), спрямований на посилення співпраці та розкриття електронних доказів, був представлений для підписання під час зустрічі, організованої Італією під час її головування в Комітеті міністрів Ради Європи. Протокол підписали держави-члени Європейської Комісії.

Угода включає засоби для зміцнення співпраці та розкриття електронних доказів, такі як: пряма взаємодія з постачальниками послуг і реєстраторами, ефективні методи отримання інформації про користувачів і трафік, негайна співпраця в надзвичайних ситуаціях або спільне розслідування з урахуванням прав людини та верховенства права, включаючи гарантії захисту даних.

Сучасні тенденції та складнощі соціальних відносин, активізація транскордонної злочинності та розвиток технологій призвели до виникнення явища, відомого як злочини у сфері інформаційних технологій. Цей сегмент практично не підлягав міжнародному правовому регулюванню протягом тривалого періоду, але на сучасний момент існують різні норми, спрямовані на протидію злочинності в цьому секторі. Слід враховувати, що наявна галузь міжнародного права не завжди є ефективною та не має єдиної системи правового регулювання в цьому контексті, що особливо проявляється у розходженні термінології та концептуальних засобах таксономії [20, с.71].

Отже, встановлення загального та уніфікованого визначення терміну «кіберзлочинність» є важливим першим кроком у розробці кримінально-правової стратегії для протидії злочинам у сфері інформаційних технологій. Незважаючи на те, що цей вид злочинів з'явився нещодавно, він став однією з найбільших загроз сучасному суспільству. Кожен рік кіберзлочинність набуває обертів і стає все поширенішою, що вимагає розробки відповідної правової теорії та методологічного інструментарію, зокрема в галузі кримінального права [77, с.168].

Більшість таких злочинів, як вказано вище, не обмежуються територіальною чи віртуальною межею конкретної країни, а можуть мати глобальний, міждержавний або навіть міжнародний характер. Це ставить під сумнів необхідність міжнародної співпраці, оскільки визначення особи злочинця, його територіального розташування та норм права, за якими може бути притягнутий до відповідальності, є складними завданнями для правоохоронців під час розслідування таких злочинів.

Для дальшого розвитку міжнародного співробітництва у протидії кіберзлочинності формулюються три основні завдання: ідентифікація особи злочинця, визначення юрисдикції та вибір найбільш ефективних юридичних заходів для його притягнення до відповідальності.

Міжнародні організації відзначають необхідність скоординованої міждержавної співпраці у розслідуванні злочинів у сфері інформаційних технологій. Зусилля Організації економічного співробітництва та розвитку (ОЕСР), Інтерполу, «Великої вісімки» (G8), Ради Європи, ООН та інших міжнародних організацій спрямовані на розвиток міжнародного співробітництва країн у боротьбі з кіберзлочинністю та формування відповідного законодавства. Проте, для ефективного використання міжнародно-правових норм необхідно мати єдиний підхід до розуміння проблем, визначення спільних завдань та формулювання загальних принципів [80, с.127].

Різні країни мають відмінний підхід до формулювання конкретних злочинів у своєму кримінальному законодавстві, що ускладнює застосування ефективних заходів протидії комп’ютерним злочинам на глобальному рівні. Тому ключову роль в координації національних кримінальних законів з міжнародними актами грають міжнародні закони та нормативні акти.

Давайте розглянемо процес розвитку міжнародно-правового співробітництва у боротьбі з кіберзлочинністю. У квітні 1995 року відбулася перша Міжнародна конференція INTERPOL з комп’ютерних злочинів. У 1996 році країни «Великої вісімки» створили спеціальну групу, що

присвячена протидії міжнародним злочинам у сфері інформаційних технологій, відому як «Ліонська група».

Одночасно лідери держав прийняли план боротьби з кіберзлочинністю. Ключові положення цього плану включають створення цілодобових контакт-центрів для співпраці у протидії злочинами у сфері інформаційних технологій, надання допомоги кваліфікованими правоохоронцями іншим країнам, розробку спільного стандарту для отримання та перевірки автентичності електронних даних, а також узгодження законодавчого підходу до боротьби з комп'ютерними злочинами в країнах-учасницях.

У 2000 році під час Десятого Конгресу з попередження злочинності та поводження з правопорушниками в рамках ООН було відзначено, що збільшення глобальної кіберзлочинності та виникнення нових форм злочинів у галузі інформаційних технологій, а також недостатня ефективність співпраці між країнами та організаціями поза межами національного та міжнародного права породжують значущі проблеми в юридичній сфері. У березні 2001 року Комісія ООН із запобігання злочинності та кримінального правосуддя вперше визначила класифікацію злочинів у сфері інформаційних технологій [82, с.396].

Окремим ключовим документом в рамках ООН є Резолюція від 2001 року «Про протидію незаконному використанню інформаційних технологій». У цій резолюції підкреслюється важливість співпраці між державою та приватним сектором для запобігання незаконному використанню інформаційних технологій, включаючи визначення відповідальності за інформаційні злочини в законодавстві, транснаціональну співпрацю правоохоронних органів, обмін інформацією для боротьби зі злочинністю, підготовку працівників правоохоронних органів до умов інформаційного суспільства, а також захист комп'ютерних систем від несанкціонованого доступу і т.д. [80].

Важливим елементом резолюції є наголошення на тому, що розвиток інформаційних технологій повинен сприяти виявленню та запобіганню

злочинному використанню, а також збору доказів. Теоретично проєкт надає правоохоронним органам інших країн можливість виявлення їх, і Організація докладає зусиль для затримання злочинців на короткі терміни, сприяючи досягненню високих результатів. Однак злочинці можуть незаконно отримати доступ до високих технологій та використовувати приховані можливості системи для вчинення злочинів у сфері інформаційних технологій, таких як викрадення персональних даних.

Ключовим актом, який унормовує міжнародну співпрацю у протидії кіберзлочинності, є Конвенція про кіберзлочинність, що була укладена в Будапешті 23 листопада 2001 року [42]. Вона встановлює загальні принципи та визначає основи заходів для протидії кіберзлочинності на національному та міжнародному рівнях.

Відповідно до положень статті 23 Конвенції, сторони максимально співпрацюють у проведенні розслідувань та судового переслідування кримінальних правопорушень, пов'язаних із кіберзлочинністю, використовуючи міжнародні документи про співпрацю в міжнародних кримінальних справах та угоди, укладені на основі єдиної або спільної внутрішньої законодавчої бази, з використанням комп’ютерних систем та даних для збору електронних доказів у зв’язку із кримінальними правопорушеннями [42].

Угода визначає чотири категорії протиправних дій щодо конфіденційності, цілісності та доступності комп'ютерних даних і систем:

1. Протиправні дії у сфері несанкціонованого доступу до інформації: незаконне перехоплення (ст. 3), втручання в дані (ст. 4), втручання в роботу систем (ст. 5), неправомірне використання обладнання (ст. 6).

2. Дії, пов'язані з незаконним використанням комп'ютерів: комп'ютерна підробка (ст. 7), комп'ютерне шахрайство (ст. 8).

3. Протиправні дії, пов'язані з контентом, включаючи виготовлення, розповсюдження та зберігання дитячої порнографії (ст. 9).

4. Правопорушення, пов’язані з порушенням авторського права і суміжних прав (ст. 10) [42].

У даному випадку виникає одна з перших труднощів міжнародної взаємодії, оскільки юридичний вплив, визначений у Конвенції, не відповідає сучасним умовам розвитку кіберзлочинності: тепер ми стикаємося не лише із самою кіберзлочинністю, але й її екстремальним виявом – концепцією кібертероризму. У відповідь на це науковці розробили класифікацію джерел кіберзлочинності, з метою оперативного виявлення загроз та вживання належних заходів для їх подолання.

З урахуванням цього фахівці розділяють особи та організації, які здійснюють атаки, на різні категорії, з яких випливає сама кіберзлочинність:

– Хакер – це особа, що має високий рівень компетенції у галузі інформаційних технологій та проводить багато часу за пристроями, виявляючи слабкі місця в інформаційних системах (здійснення злочинних дій, таких як: атаки типу DoS, дефейс, розповсюдження шкідливих програм і т.д.).

– Хактивісти, які поєднують соціальну активність з напрямом проти чогось та використанням інтернет-технологій для завдання шкоди комп’ютерним мережам та їх користувачам. Їхню діяльність характеризують злочини, такі як: поширення шкідливих програм (вірусів), особисті образи та брехня.

– Злочинці, чиє заняття спрямоване на неправомірне здобуття вигоди (крадіжка банківських карт, фішинг, інтернет-шахрайство і т.д.).

– Професіонали, які займаються промисловим шпигунством.

– Кібертерористи, чия діяльність пов'язана з різними виявами екстремізму в мережі. Сучасні терористи можуть використовувати Інтернет (самостійно чи в поєднанні з фізичними атаками) як інструмент для завдання реальної шкоди [5, с.14].

Важливим аспектом, на який слід звернути увагу при розгляді Конвенції, є акцент на участі в кіберзлочинах, визначаючи відповідальність

за замах і пособництво (ст. 11) та колективну відповідальність за співучасть (ст. 12). Щодо покарання за вчинення цих злочинів, стаття 13 Конвенції зобов'язує кожну державу вживати належних законодавчих та інших заходів для забезпечення ефективних, пропорційних і переконливих санкцій, включаючи позбавлення волі, для кримінальних порушень, передбачених статтями 2-11 Конвенції.

Також підкреслюється, що відповідальність юридичних осіб повинна забезпечуватися на підставі ефективних, пропорційних і переконливих кримінальних або некримінальних санкцій, включаючи фінансові штрафи. Згідно зі статтею 15 Конвенції, країни-учасниці повинні забезпечити встановлення, виконання та застосування повноважень і процедур, визначених у Конвенції, відповідно до умов і гарантій, установлених національним законодавством для забезпечення повного захисту прав і свобод людини [42].

Конвенція передбачає ряд запобіжних заходів]:

– Загальні заходи, включаючи термінове збереження комп'ютерних даних (ст. 16), негайне збереження та часткове розкриття даних про рух інформації (ст. 17).

– Заходи доручення (ст. 18), які встановлюють процедури та обмеження для видавання відповідних доручень правоохоронним органам інших країн для проведення необхідних процесуальних дій на їхній території.

– Обшук та вилучення збережених комп’ютерних даних (ст. 19).

– Збір комп’ютерних даних у режимі реального часу, включаючи отримання даних про рух інформації в реальному часі (ст. 20) та перехоплення даних інформаційного змісту (ст. 21).

Щодо міжнародного співробітництва у сфері прямої боротьби з кіберзлочинцями, Конвенція встановлює наступні заходи [42]:

– Видача (ст. 24): механізм, що дозволяє передати особу, звинувачену у кіберзлочині, для проведення судового розгляду.

– Взаємна допомога (ст. 25): обидві сторони надають взаємну допомогу для розслідування чи судового переслідування кіберзлочинів та збору електронних доказів.

– Добровільна допомога (ст. 26): передача інформації, яка може сприяти розслідуванню кіберзлочинності без попереднього запиту.

– Взаємна допомога щодо тимчасових заходів (ст. 29 та 30): термінове збереження та розкриття збережених даних.

– Взаємна допомога щодо слідчих повноважень (ст. 31-34): взаємна допомога в доступі до комп'ютерних даних, транскордонний доступ до відкритих даних, збір даних потоку в реальному часі та перехоплення інформаційних даних.

– Цілодобова мережа (ст. 35): створення та утримання мережі для обміну інформацією про запобігання кіберзлочинам [42].

Аналізуючи питання боротьби з кіберзлочинністю за допомогою Конвенції, можна зробити висновки щодо загальних позицій стосовно криміналізації дій, пов'язаних із використанням комп'ютерних систем. Зокрема, визначено, що такі дії вважаються кримінальними, що виправдовує застосування необхідної сили для ефективної боротьби з ними, а також вживання заходів для виявлення, розслідування та судового переслідування таких злочинів на рівні як в межах країни, так і на міжнародному рівні.

По-перше, наявність визначень у Конвенції, що стосуються «пошуку та конфіскації збережених комп'ютерних даних», дозволяє одній стороні забезпечити збереження важливої інформації, необхідної для розслідування злочину, що опинився в юрисдикції іншої сторони. Інтернет-провайдери часто володіють даними про минулі обміни інформацією, які можна отримати за допомогою спеціального обладнання, що реєструє конкретні аспекти обміну інформацією, включаючи час, тривалість і дату будь-яких повідомлень. Такі дані зазвичай зберігаються обмежений період часу, з урахуванням комерційних потреб оператора чи постачальника послуг, а

також вимог законодавства, що регулює нерозголошення приватної інформації.

Важливою характеристикою Конвенції є можливість вживання правових та інших заходів для надання компетентним органам повноважень конфіскувати або захищати дані від знищення, що стає необхідним для проведення розслідувань та досліджень [42]. Юридично обґрунтовані загальні принципи міжнародного співробітництва, закріплені в Конвенції, виявляються вельми важливими. Співробітництво щодо екстрадиції злочинців у сфері інформаційних технологій, широка взаємна допомога у розслідуванні кримінальних справ, пов'язаних із комп'ютерними системами та даними, та збір електронних доказів стають менш вірогідними, оскільки кіберзлочинність вже не обмежена територією однієї країни, враховуючи специфіку цього явища та глобальний характер Інтернету.

У процесі проведення розслідувань правоохоронні органи різних країн повинні взаємодіяти, використовуючи формальні структури, такі як Інтерпол, або неформальні, передаючи корисну інформацію національним правоохоронним органам. Виникають додаткові питання, коли мова йде про правову допомогу у розслідуванні злочинів у сфері інформаційних технологій. Якщо внутрішнє законодавство країни не встановлює конкретні повноваження для отримання доказів в інформаційних мережах, такі сторони не можуть ефективно реагувати на запитання іншої сторони про допомогу [39, с.45].

Таким чином, важливою умовою міжнародного співробітництва є координація всіх сторін для вжиття необхідних заходів у розслідуванні злочинів у сфері інформаційних технологій. Варто відзначити, що деякі країни Західної Європи застосовують правовий принцип, згідно з яким країна може встановлювати юрисдикцію над територією іншої країни у разі порушення інтересів останньої. Однак в Європейському союзі висловлюється обурення, що цей принцип вимагає міжнародного регулювання, оскільки країни часом тлумачать його надто широко.

В сучасний час пріоритетним завданням міжнародного співробітництва є уніфікація національного кримінального законодавства країн, що беруть участь у міжнародному співробітництві у сфері протидії кіберзлочинності, навіть при існуванні конвенцій. Зростання рівня кіберзлочинності та відсутність ефективного соціально-правового контролю представляють серйозну загрозу для сучасної цивілізації.

Ці виклики можливо подолати лише шляхом впровадження комплексної стратегії боротьби із цим видом кіберзлочинності, яка обов'язково включатиме кримінально-правові та судові підходи. Важливою складовою цієї стратегії буде підвищена міжнародна співпраця, оскільки транснаціональні аспекти кіберзлочинності та кібертероризму неможливо ефективно контролювати на рівні окремих країн. У XXI столітті міжнародному співтовариству необхідно терміново зайнятися вирішенням цього складного завдання [66, с.196].

Враховуючи вищезазначені аспекти, можна узагальнити, що створення та розвиток міжнародного співробітництва в сфері протидії кіберзлочинності спрямовані на вирішення трьох ключових завдань: ідентифікація особи порушника, встановлення юрисдикції та, головне, вибір належного правового впливу на порушника, який найбільш адекватно викличе у нього відчуття провини за скоєння цього злочину та схожих.

РОЗДІЛ 3
ВИКЛИКИ ТА ПЕРСПЕКТИВИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

3.1. Загрози кіберзлочинності в XXI столітті

Протягом XXI століття відбувся значний технологічний прогрес, який вплинув на спосіб життя людства. Проте, цей інноваційний розвиток також породив новий клас загроз – загрози кібербезпеки. Реалізація ефективної політики кібербезпеки та протидія кіберзлочинності стають складними через ряд унікальних факторів.

По-перше, кіберзлочинність, за своєю природою, не обмежена кордонами та швидко розвивається, випереджаючи реакцію національних та міжнародних владних структур.

По-друге, горизонтальна характеристика кіберзлочинності робить можливим вчинення практично будь-якого злочину через мережу Інтернет. Додатково, збір доказів для таких незаконних дій ускладнений нестабільністю електронних даних та потребою в глибоких знаннях для їх обробки.

По-третє, для ефективного збереження електронних доказів та їхньої допустимості в судовому процесі потрібне тісне міжнародне судове співробітництво. Однак, це часто ускладнюється значними відмінностями у правових системах країн та конфліктами юрисдикцій. Динамічний характер кіберпростору, який постійно змінюється та залежить від світових тенденцій і локальних геополітичних факторів (наприклад, активізація кіберзлочинців під час пандемії COVID-19), додає до цього викликів.

Кіберзлочин містить незаконне отримання доступу до електронної системи, незаконне проникнення в неї або незаконну взаємодію з іншою електронною системою. Деякі кіберзлочини представляють собою новий спосіб вчинення традиційних злочинів проти власності, таких як крадіжка та

шахрайство, або злочинів проти особистості, таких як переслідування та напад [67].

Інші кіберзлочини вчиняються з можливістю використання електронної системи, наприклад фішинг та хакерство. Країни та транснаціональні корпорації, які прагнуть захистити свої електронні системи від серйозних загроз, намагаються сформувати закони, які б карали та невиправдовували найсерйозніші злочини, скоєні за допомогою електронних систем [67].

Кіберзлочинність у новому столітті є постійною загрозою. Коли поліція та прокуратура припиняють один вид онлайн-злочинів, інший з'являється. Визначення та застосування кримінального законодавства можуть бути нечіткими і національні держави можуть не мати можливості покарати осіб за ці злочини, які просочуються через юридичні прогалини. Крім того, коли злочинна поведінка розповсюджується в електронному просторі, електронне з'єднання може перетнути міжнародні кордони, що призводить до суттєвих проблем з юрисдикцією.

Універсальна юрисдикція дозволяє одній нації вживати заходів для покарання правопорушників, які проживають за межами її територіальних кордонів, за вчинення злочинів у власній країні. Проте, визначення і застосування принципів універсальної юрисдикції до кіберзлочинності залишається складним. Кіберзлочини часто вчиняються анонімно, ускладнюючи виявлення їх виявлення з двох причин. Навіть якщо кіберзлочин буде виявлено в межах певної юрисдикції, яка вирішила розпочати розслідування, ідентифікація, арешт та переслідування порушників за межами кордонів країни може бути вкрай складними.

Потенційна кількість постраждалих від кіберзлочинності майже необмежена, а фактична кількість жертв залишається невідомою. Навіть при тому, що потенційний вплив кібервіктимізації значний (збитки оцінюються мільярдами або трильйонами доларів щорічно), компанії та країни можуть приховувати інформацію про комп’ютерні вторгнення, щоб уникнути коливань на фондовому ринку або уникнути паніки серед громадськості.

Деякі особи, зокрема молодь, можуть навіть не усвідомлювати, що стали жертвами кіберзлочинців, або вони можуть не бажати повідомляти про особисті випадки віктимізації своєму оточенню. Таким чином, рівень реальної віктимізації встановити неможливо [84].

Тепер прийшов час розглянути можливість застосування принципів кримінальної юрисдикції для компенсації більш широкого спектру онлайн-жертв. Для цього необхідно розглядати кіберпростір як фізичну реальність. Навіть якщо взаємодія через Інтернет здійснюється через різні країни, якщо правопорушник і жертва фізично прив'язані до однієї національної держави, то закони цієї держави повинні мати чинність для вирішення правопорушень.

Якщо жертва і правопорушник представляють різні країни, необхідно адаптувати юрисдикційні закони для можливості переслідування правопорушників у будь-якому місці. У традиційних сценаріях припускалося, що злочинець і його жертва перебувають у фізичному контакті один з одним.

Проте, це припущення втрачає свою актуальність у випадку кіберзлочинів, де злочинець може знаходитися в будь-якому місці. Закони різних юрисдикцій ускладнюють цю ситуацію. Деякі країни можуть не визнавати комп'ютерні «правопорушення» і можуть відмовлятися екстрадувати свого громадянина в іншу країну, яка вважає цю діяльність незаконною.

Закони, що стосуються традиційної власності, можуть бути недостатніми і неефективними в кіберпросторі. Без фізичної присутності, наприклад, віртуальний доступ до комп'ютера чи спроба отримати доступ до іншого комп'ютера без авторизації, може не порушувати закони багатьох юрисдикцій. Інтернет дозволяє людям взаємодіяти будь-де, будь-коли і будь-яким чином. Поширення Інтернету спонукає нас реагувати та думати творчо, оскільки комп'ютери використовуються злочинцями для завдання особистої та фінансової шкоди [11, с.138] .

Область кібербезпеки продовжує страждати від серйозного дефіциту кваліфікованих фахівців, а експерти попереджають, що ставки надто високі, оскільки епідемія кіберзлочинності навіть загрожує підірвати віру суспільства в такі цінності, як: демократія і особиста конфіденційність.

Крім того, розвиток цифрових технологій створює серйозні виклики, щодо забезпечення необхідного рівня цифрової безпеки як на рівні країни в цілому, так і для окремих підприємств. При цьому, із впровадженням цифрових технологій у бізнес-процеси, проблема кібербезпеки стає вкрай актуальною, адже кіберзлочини та хакерські атаки можуть мати не тільки локальні, а й глобальні наслідки, включаючи вплив на людські життя та можливі різновекторні катастрофи.

Багато підприємств ігнорують загальну картину цієї проблеми через невідповідність їхніх знань та досвіду у цій області. Ті підприємства, що застосовують заходи з кібербезпеки, часто використовують застарілі методи, що не відповідають поточним викликам сучасності. Отже, із зростанням використання цифрових технологій, виникає необхідність в оцінці рівня кібербезпеки, що тепер розглядається як необхідний елемент загальної економічної безпеки підприємства [53].

У світлі цього, кібербезпека підприємства виходить на новий рівень, оскільки вона охоплює не лише захист інформації, але й важливі аспекти, такі як: захист іміджу та репутації, збереження довіри споживачів та клієнтів, фізична та фінансова безпека. Задачею також стає збереження ринкових переваг та протидія недобросовісній конкуренції [17, с.206].

Враховуючи зазначені фактори, важливим стає впровадження кібернавчання серед персоналу, оскільки методи соціальної інженерії, які часто використовуються кіберзлочинцями, базуються на низькій цифровій грамотності робітників. Це стає слабкою ланкою в будь-якій системі кібербезпеки підприємства, навіть у розвинутій. Проте, виникає проблема дефіциту кіберспеціалістів, оскільки більша частина навчання фокусується на

промисловій безпеці, майже ігноруючи інформаційну та цифрову безпеку [58, с.77].

Однією з найбільших вразливостей, якою користуються злочинці, є застаріле програмне і антивірусне забезпечення. Багато підприємств, особливо поза галуззю IT, не розглядають оновлення програмного забезпечення як необхідне, використовуючи застарілі операційні системи. Це створює додаткові кіберризики для всього підприємства, оскільки застарілі системи не можуть ефективно протидіяти сучасним кіберзагрозам та викликам.

На додаток до цього, підходи керівництва за принципом «не треба змінювати, поки працює», блокують розвиток компанії та створюють значні ризики. Цей архаїчний підхід обмежує як кібербезпеку, так і загальну економічну безпеку підприємства, оскільки застарілі системи не здатні адаптуватися до сучасних викликів та загроз. Разом із активним впровадженням цифрових технологій неодмінно виникає ряд нових викликів та можливостей, серед яких важливе місце займає стрімкий розвиток галузевого програмного забезпечення [60].

Це програмне забезпечення, поступово інтегруючись з іншими сервісами та ресурсами, стає ускладненим та надзвичайно вразливим перед загрозами кіберзлочинності. Супроводжує цей процес також стрімке зростання кібератак, внаслідок чого збільшується відповідальність розробників програмного забезпечення за ефективний захист від нових загроз та шкідливих атак.

Зі збільшенням ризиків, пов'язаних із кіберзагрозами, виникає необхідність вдосконалення систем кібербезпеки, що набуває великого значення при оцінці рівня економічної безпеки підприємства. Цифрова трансформація підприємства та його виробничих процесів стає невідємною частиною сучасного бізнес-середовища, а ефективність цього процесу прямо залежить від надійності системи кібербезпеки.

У контексті цифрової трансформації економіки дуже важливим стає питання кіберзахисту критичної інфраструктури та розвитку політики щодо підвищення рівня цифрової грамотності населення. Протистояння кіберзагрозам у реальному часі стає ключовим аспектом, який суттєво впливає на рівень кібербезпеки підприємства. Тому розробка ефективних методів та підходів до боротьби з кіберзлочинністю має визначити сучасні підприємства як пріоритетний напрямок їхнього розвитку в умовах активної цифровізації [79, с.12].

До того ж, варто звернути увагу і на той факт, що розробники та оператори телекомунікаційного обладнання у світлі викликів нового етапу готові значно модернізувати архітектуру мереж та принципи їх взаємодії. Цей рух призвів до виникнення мереж п'ятого покоління (5G), що є наступним етапом у розвитку четвертого покоління мереж (LTE, 4G) [25, с.118].

Стандарт 5G визначає новий вимір розвитку бездротових технологій, обіцяючи необмежений доступ до мережі для користувачів і різних пристроїв [26, с.32]. Розробка 5G включає в себе нові архітектурні концепції та можливості для створення нових бізнес-моделей, а також розширює спектр програм і послуг для абонентів. Це представляє собою повноцінне поєднання удосконалених бездротових технологій та додаткових функцій. Швидкість передачі даних в 5G-мережах не лише покращить якість надання послуг, але й розширить можливості для онлайн-бізнесу. Прогнозується, що швидкість 5G досягатиме 10 Гбіт/с [27, с.53].

При взаємодії Internet of Things з мережами 5G, які представляють собою майбутнє покоління, багато пристроїв отримують сенсори та додаткові модулі, що надає їм здатність обробляти та передавати інформацію без прямого втручання людини. Із використанням високошвидкісних мобільних мереж нового покоління, загрози інформаційної безпеки для державних та приватних установ збільшуються, оскільки мережі 5G сприяють розширенню об'єктів, привабливих для організації кібератак. Це відкриває для

зловмисників більше технічних можливостей, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи, а не лише для комунікації.

Зі збільшенням швидкості передачі даних у мережах 5G збільшуються шанси зловмисників впроваджувати компактні шкідливі коди або залишати менше слідів при перехопленні трафіку. Застосування цих технологій у роботі працівників, зокрема використання мобільних пристроїв для віддаленої роботи, робить інформаційні системи більш вразливими перед потенційними кіберзагрозами. Зокрема, розвиток мереж 5G викликає потребу у вдосконаленні заходів інформаційної безпеки та розробці нових стратегій для запобігання кібератак в умовах зростаючого обсягу обміну даними в мережах майбутнього.

Наприклад, нові фактори загроз можуть виникнути у зв'язку із поширенням Ransomware, відомого як трояни-вимагачі. В сучасний період ці зловмисники можуть не лише блокувати файли на комп'ютері або смартфоні користувача, але також в майбутньому можуть розширити свою діяльність на фізичний світ, особливо в епоху «Інтернету речей». Наприклад, троянець може заблокувати доступ до особистого будинку, офісу чи навіть автомобіля. Зростання кількості підключених пристроїв може значно полегшити створення потужних ботнетів для DDoS-атак, зокрема через підключення мільярдів нових пристроїв, більшість з яких є домашніми пристроями, що контролюються звичайними людьми [28].

Поява 5G мереж представляє нові виклики для кібербезпеки, оскільки такі мережі будуть більш складними та динамічними порівняно з попередніми поколіннями мобільних мереж. Наприклад, нові віртуалізовані мережеві вузли можуть додаватися та видалятися з мережі в будь-який час. Для ефективного виявлення та відстеження векторів загроз та атак, а також забезпечення необхідного рівня довіри, 5G мережі повинні бути спроєктовані з врахуванням структурованого підходу, який включає необхідні механізми захисту та їх повне охоплення [26].

Варіант концепції для забезпечення безпеки в мережах 5G базується на детальному аналізі трафіку мобільної передачі даних та SMS-трафіку на рівні оператора. Основна мета полягає у виявленні активності, що є характерними для шкідливого програмного забезпечення, а також виявленні нестандартних моделей використання пристроїв, зокрема смартфонів і планшетів [26].

Ключовим аспектом є обмін інформацією щодо небезпек, порушень та пов'язаних рішень. Цей обмін повинен бути відкритим і здійснюватися не лише з клієнтами та партнерами, але й з регулюючими органами та можливо навіть з конкурентами. Відкритість є необхідною, оскільки всі сегменти мережі піддаються кіберзагрозам.

Вимоги до системи безпеки повинні базуватися на кількох аспектах:

– забезпеченні захисту доступу до мережі;
– використанні додатків, що гарантують безпечну роботу в мережі;
– існуванні вбудованої служби безпеки;
– передачі автентичних і цілісних даних з урахуванням збереження їх конфіденційності.

Деякі класи управління безпекою надають структурований підхід для запобігання або відповіді на конкретний ризик, пов'язаний із конкретними даними, функціями та послугами в мережі. Визначені сфери безпеки націлені на задоволення потреб одного чи декількох рівнів або доменів, групуючи різноманітні аспекти мережі, які є специфічними для конкретної області.

Розподіл сфер безпеки відносно функціональності, доменів, верств і кінцевих точок протоколів визначає вибір механізмів контролю за безпекою для кожного підрозділу, що надає детальний огляд механізмів безпеки, що потрібні в мережі 5G. Забезпечити безпечне підключення до мережі можна за допомогою служби перевірки автентичності мережі та користувача, криптографічних ключів та ідентифікаторів додатків [26].

Швидка реакція на загрози безпеки вимагає наявності мережевої архітектури, що є багатомірною та цілісною, об'єднуючи безпеку, приватність та події, які виникають в мережі. Архітектура безпеки повинна

охоплювати всі нові технології та концепції, що використовуються в 5G, які є значущими етапами еволюції від 4G. Система 5G сильно покладається на захист і віртуалізацію мережі для підвищення гнучкості та масштабованості.

3.2. Перспективи міжнародної боротьби з кіберзлочинністю

Аналізуючи розвиток кіберпростору, можна виділити кілька важливих тенденцій, які значно вплинуть на його функціонування у найближчому майбутньому. Перша тенденція полягає в тому, що інформаційна безпека тісно пов'язана із кібербезпекою, що реалізується у кіберпросторі. Наявність кіберпростору значно впливає на інформаційну сферу будь-якої країни.

Кіберпростір розглядається як частина національної інфраструктури, що вимагає системи безпеки на рівні інших елементів державної інфраструктури. Однією з основних проблем кіберпростору є забезпечення безпеки циркулюючої інформації та стійкість національного сегменту до кібератак. Інформаційна зброя змішує межі між військовими та цивільними об'єктами через тісний зв'язок між військовими та цивільними інформаційними інфраструктурами. В майбутньому цивільні інформаційні системи можуть стати головним об'єктом атаки з боку потенційного противника [4, с.17].

Тенденція друга полягає в тому, що кіберпростір поступово перетворюється на п'ятий сектор військових дій. Крім традиційних секторів (наземний, морський, повітряний, космічний), кіберпростір стає новим майданчиком для військових дій. Тут планується участь не лише військ, але й спецслужб країни, хакерів та всіх, хто може використовувати інформаційні технології для ведення війни.

У сучасному світі деякі країни, зокрема США і Китай, реалізують активну державну політику, розглядаючи кіберпростір як нове поле бою. Вони вкладають значні зусилля у встановлення повного контролю над цим простором і створення засобів для його ефективного управління. Така стратегія вже має численні прецеденти, де інформаційна зброя

використовувалася в усіх військових конфліктах останніх двадцяти років, стаючи невід'ємною частиною арсеналу Китаю, США та їх союзників.

На сьогодні існує понад 120 країн, які активно розвивають потенціал інформаційного протиборства. Це свідчить про значний рівень інтересу до цього напряму, порівняно з розробками у сфері ядерної зброї, які ведуть менше ніж 20 країн. Загальний наратив також орієнтується на те, що майбутні війни будуть вестися в онлайн-режимі, використовуючи вразливості комп'ютерних систем інфраструктури та соціальних мереж для руйнування і створення паніки серед населення [85, с.2].

Трансформація військової інформаційної архітектури вже відбувається, де традиційні збройні сили «інформатизуються», а озброєння «інтелектуалізується». Розвиток концепції ексцентричного ведення бойових дій вказує на стратегію забезпечення переваги над противником шляхом ефективного збору, обробки та використання інформації. Сучасні розробки високочастотної електромагнітної імпульсної зброї, яка може виводити з ладу електроніку в радіусі сотень кілометрів, стають складовою тактичного визначення інформаційної зброї в ряді розвинених країн. Експерти підкреслюють, що ці можливості вже доступні для використання в деяких країнах.

В момент найновіших технологічних досягнень розробляється мікрохвильова зброя великої потужності, спроможна змінювати траєкторію ракет у польоті. Ця зброя може викликати перевантаження, виводити з ладу мережі зв'язку та електроніку систем озброєння. Також вона здатна вражати екрановані приміщення, захищені від радіоактивного випромінювання, завдаючи збитків здоров'ю та життю осіб, що перебувають в радіусі дії цієї зброї [84].

Одночасно намітилася тенденція до формування військово-мережевого комплексу для забезпечення переваги у кіберпросторі. У період «холодної війни», коли розгорнулася «гонка озброєнь», США та СРСР створили військово-промислові комплекси, спрямовані на виробництво озброєння та

військової техніки. Сьогодні вони розглядаються як сукупність підприємств та організацій, що виробляють озброєння для збройних сил своєї держави та на експорт. В Україні та Росії цей термін замінено на «оборонно-промисловий комплекс», що відображає спільні інтереси влади, воєнно-промислових корпорацій і вищого командного складу.

Військово-промисловий комплекс це явище, яке базується на збігу інтересів воєнно-промислового керівництва, вищого командного складу та держави. Його проявами є лобіювання інтересів воєнної промисловості на державному рівні та підвищення її впливу на суспільні процеси. Спектр його галузей включає ракетно-космічну, авіаційну, суднобудівну, бронетехнічну, радіоелектронну та артилерійсько-стрілецьку галузі.

Нинішні події в області інформаційного протиборства та кіберпростору схожі на витоки створення військово-мережевого комплексу, де інтереси та можливості спецслужб і військового сектору сплітаються з інтересами та можливостями приватних структур, що суттєво змінює сам кіберпростір і характер його воєнних дій.

Щоб вирішити це завдання, відбувається взаємодія державних структур із технологічним сектором Інтернету, включаючи провідних виробників мікроелектроніки, обчислювальної та телекомунікаційної техніки для збору інформації про користувачів. Засоби масової інформації неодноразово повідомляли про співпрацю із спецслужбами таких великих виробників, як: Cisco, Huawei, Crypto AG, Microsoft, Facebook та інші. Ця співпраця навіть включає в себе вбудовування необхідних бекдорів та передачу таємних вразливостей спецслужбам в апаратному та програмному забезпеченні [84].

Четверта тенденція полягає в тому, що проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу призводять до перерозподілу повноважень між існуючими учасниками в сфері захисту інформації. Виявлено, що державні органи не будуть визначальними гравцями в цій сфері, і їхні обов'язки обмежаться стратегічним управлінням та встановленням стандартів безпеки. Ключові

об'єкти інфраструктури отримають відповідальність за їхню реалізацію і бізнес-корпорації, завдяки своїм ресурсам та експертизі, будуть основними виконавцями цих завдань. Вони будуть розробляти та впроваджувати методи виявлення шкідливих програм та хакерської активності на основі даних, які вони збиратимуть в режимі реального часу у своїх інформаційних мережах та мережах клієнтів.

П'ята тенденція полягає в тому, що надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу. Ці організації не тільки розслідують вже здійснені вторгнення, але також пропонують послуги із захисту мереж від потенційних загроз. Вони будуть створювати кіберармії та навчати їх воювати в мережі, що може призвести до їхньої інтеграції в арсенал збройних сил країни. Для ефективного протистояння щоденним кіберзагрозам виникає необхідність у створенні безпечних зон Інтернету, що представлятимуть собою повноцінні кібернетичні інфраструктури, де безпека стане головним пріоритетом. В таких «екозонах безпеки» трафік буде більш активно та ретельно аналізуватися, відзначаючи їх як онлайн аналоги особливо охоронюваних територій.

Підняття рівня кібербезпеки стане привабливою споживчою якістю, яка привертає увагу клієнтів. Компанії, що візьмуться за створення та обслуговування таких захищених кіберзон (інтернет-провайдери, банки та інші, що працюють із персональними даними), будуть залучати найбільш досвідчених та кваліфікованих співробітників, оскільки рівень зарплати у них буде значно вищий, ніж у секторі державної чи військової справи [85].

Такі інфраструктури можуть обмежувати їх використання, встановлювати правила та вимоги, а також пропонувати особливі переваги, зокрема щодо безпеки. В рамках таких мереж буде ретельно аналізуватися трафік на предмет шкідливих програм, висилатися попередження про потенційні загрози особовим даним, проводитися контроль намагань ввійти до мережі та уникати будь-яких підозрілих користувачів.

Також варто відзначити, що у державному та військовому секторах багатьох країн використовуються комерційні програмні продукти, які мають недоліки в захисті і можуть зробити обороноздатність країни вразливою для кібернетичних атак противника, представленого його військовими, спецслужбами, хакерами та терористами.

З 2021 року країни-члени Організації Об'єднаних Націй беруть участь у переговорах щодо розробки угоди, спрямованої на запобігання злочинному використанню інформаційно-комунікаційних технологій, відомої як оновлена Конвенція ООН про кіберзлочинність. Ця угода може визначити глобальну політику стосовно кіберзлочинності та поліпшити міжнародне співробітництво. Вона також може розширити повноваження національних правоохоронних органів у розслідуванні та протидії кіберзлочинам.

Однак без достатніх гарантій прав людини, ця угода може становити ризик для прав та свобод. Її розробка повинна враховувати гарантії прав людини, щоб уникнути ненавмисного узаконення розширення державного контролю над онлайн-контентом. Це може зашкодити свободі слова та змінити доступ правоохоронних органів до даних, порушуючи право на приватне життя та інші основні права [84].

Зусилля щодо покращення міжнародного співробітництва у боротьбі з кіберзлочинністю повинні бути спрямовані на забезпечення підзвітності, при цьому дотримуючись процесуальних захистів та не порушуючи право на конфіденційність. Одним із прикладів є Закон США про роз'яснення законного використання даних за кордоном 2018 року, проти якого виступили Human Rights Watch та інші групи громадянського суспільства, і який змінив систему транскордонного доступу до даних у кримінальних розслідуваннях [84].

Він надає владі США повноваження наказувати постачальникам послуг США передавати інформацію, незалежно від місця зберігання та дозволяє правоохоронним органам однієї країни безпосередньо обслуговувати запити на виробництво даних, таких як: вміст електронної пошти, або здійснювати

прослуховування на міжнародному рівні без контролю за країною, де відбувається втручання, після укладення угоди між США та іншою країною.

Другий додатковий протокол до Будапештської конвенції, який визначає нові правила щодо посиленого міжнародного співробітництва та доступу до доказів у хмарному сховищі, зазнав критики від Electronic Frontier Foundation, міжнародної групи цифрових прав, через відсутність достатніх гарантій конфіденційності та накладення обмежень на збір даних правоохоронними органами. Протокол може поставити під загрозу користувачів технологій, журналістів, активістів і вразливі верстви населення в країнах із слабким захистом конфіденційності та послабити право кожного на конфіденційність і вільне вираження поглядів у всьому світі.

Багато урядів також мають намір спростити екстратериторіальний доступ правоохоронних органів до даних. Наприклад, Міністерське розпорядження Індонезії вимагає від усіх приватних постачальників цифрових послуг і платформ, включаючи іноземні компанії, забезпечувати правоохоронним органам доступ до електронних даних для кримінального розслідування будь-якого злочину, за який передбачено покарання у вигляді позбавлення волі не менше двох років[84].

Регламент також передбачає, що компанії повинні надавати доступ як до своїх «систем», так і до своїх «даних» для цілей «нагляду» щоразу, коли це вимагається від влади. Надання владі прямого доступу до значних обсягів інформації, яку збирають і зберігають приватні компанії, є явним ризиком для прав людини. Такими вимогами особливо легко зловживати, обходячи ключові процедурні гарантії та можна легко виходити за межі того, що можна вважати необхідним і пропорційним.

Багатосторонні переговори часто виключають громадянське суспільство та інших правозахисників, особливо в справах, що стосуються діяльності правоохоронних органів. Хоча на засіданнях комітетів Ради Європи зазвичай запрошують громадянське суспільство для участі у розробці проєктів для пленарних засідань, це не стосувалося переговорів щодо Другої

додаткової конвенції, навіть після того, як майже 100 організацій закликали до більшої прозорості у цьому процесі. Процес також не забезпечив достатньо часу для розгляду ключових положень, що стосуються гарантій захисту даних[84].

Організація Об'єднаних Націй також має ситуації щодо незалучення неурядових груп до обговорень, включаючи відмову у наданні акредитації правозахисним організаціям та блокування груп у їхніх виступах. У недавньому процесі ООН з кібербезпеки були відхилені запити правозахисних груп, аналітичних центрів, компаній та інших стосовно участі через непрозоре урядове вето.

Проте, пізніше уряди погодились, що неурядові групи, акредитовані в ООН, матимуть можливість брати участь, а інші зацікавлені сторони можуть бути спостерігачами, якщо уряди не заперечують. Для неурядових організацій, навіть, таких як Human Rights Watch, буде важливо прискорити розгляд цього питання та активно брати участь у переговорах, виступаючи проти будь-якого результату, який негативно впливає на права людини.

Для урядів держав, які дотримуються принципів прав людини і не вважають ООН універсальною організацією, яка має займатись викликами кіберзагроз, також важливо забезпечити, достатню кількість представників, які будуть активно вести переговори та голосувати відповідно до своїх зобов'язань щодо прав людини та виступати проти будь-яких угод, які несумісні з цими принципами.

Для узгодження багатосторонніх договорів можуть знадобитися роки, а для набуття чинності – навіть більше. Також немає гарантії, що дві третини урядів коли-небудь досягнуть згоди щодо ухвалення угод. Замість укладення глобальної угоди, існують заходи, які уряди можуть та повинні вжити для боротьби з кіберзлочинністю. Наприклад, вони можуть підтримувати та використовувати договори про взаємну правову допомогу та інші угоди для забезпечення вищого рівня захисту прав під час обробки запитів на транскордонний доступ до даних.

Інвестиції в розбудову спроможності правоохоронних органів, прокуратури та судової системи з дотриманням прав, підвищення ефективності, прозорості та захисту прав у запитах правоохоронних органів на дані для розслідувань, а також технічна допомога країнам, які борються з кіберзлочинністю, можуть значною мірою допомогти підтримувати права під час боротьби зі злочинністю.

Ще одним ключовим заходом є виділення більше ресурсів на посилення безпеки та захисту навколо систем, вразливих до атак. Обмеження збору та зберігання даних необхідних виключно для законної мети, обмежило б вразливість людей до цифрових загроз. Боротьба зі зростаючою загрозою кіберзлочинності, одночасно захищаючи права, є актуальною проблемою, яку небагатьом урядам вдається правильно вирішити .

Існує реальний ризик того, що спроба домовитися про угоду ООН щодо боротьби з кіберзлочинністю в поляризованому середовищі, стане неможливою через відсутність політичної волі та бажання поставитися до проблеми серйозно. Інвестиції в альтернативи захисту прав – це правильний шлях [82, с.397].

Таким чином, перспективи міжнародної боротьби з кіберзлочинністю визначаються необхідністю ефективного співробітництва та введенням конкретних стратегій на глобальному рівні. Врахування швидкого розвитку технологій та зростаючої загрози кіберзлочинності визначає необхідність адаптації міжнародних структур та законодавства до сучасної динаміки цього цифрового виміру.

Прозорість та обмін інформацією між країнами вважаються ключовими аспектами ефективного протидії кіберзлочинності. Створення єдиної платформи для обміну найкращими практиками, технічними засобами та даними про загрози сприятиме вдосконаленню реакції на кібератаки. Однак, важливо враховувати права людини та приватність у процесі боротьби з кіберзлочинністю. Забезпечення балансу між безпекою та основними

свободами громадян вимагає розробки міжнародних стандартів, які будуть визначати рамки дій для кожної країни.

Крім того, надзвичайно важливим є залучення не тільки урядових структур, але й приватного сектору, академічних груп і громадянського суспільства. Спільна робота різних суб'єктів сприятиме створенню комплексної системи захисту, враховуючи різноманітність кіберзагроз та шляхи їх нейтралізації. Національні та міжнародні правові рамки повинні стати більш адаптованими до викликів кіберпростору, а їх виконання має супроводжуватися ефективним механізмом відповідальності за порушення.

Загалом, міжнародна боротьба з кіберзлочинністю вимагає гнучкості, інновацій та гармонізації зусиль різних країн для створення стійкого та безпечного кіберсередовища.

ВИСНОВКИ

На підставі проведеного дослідження, можемо зробити ряд висновків:

1. Сучасний кіберпростір є не лише ареною глобальних конфронтацій, але й можливим підґрунтям для ініціаторів кіберзагроз з боку різних міжнародних акторів. Держави, недержавні суб'єкти та кіберзлочинці використовують передові технології для реалізації своїх стратегічних цілей, нерідко виходячи за межі національних кордонів та порушуючи цілісність інших країн.

Швидкий розвиток технологій дозволяє міжнародним акторам вести інформаційні операції, спрямовані на розкол та дестабілізацію інших країн. Ескалація конфліктів у кіберпросторі не лише підриває міжнародний порядок, але й покладає під загрозу кібербезпеку та економічну стабільність багатьох держав. Такі дії викликають необхідність пошуку колективних рішень та встановлення міжнародних стандартів у галузі кібербезпеки. Відсутність єдиного підходу та взаємодії в цьому питанні може призвести до подальшого поглиблення проблем та загострення конфліктів у кіберпросторі.

Отже, для забезпечення стійкості та безпеки у кіберпросторі важливо не лише визнавати існуючі загрози, але й активно працювати над спільними стратегіями, що дозволить вирішувати проблеми на міжнародному рівні та запобігати подальшій ескалації кіберзагроз.

2. Дослідження понять «кібербезпека» та «кібербезпекова політика» вказав на їхню динамічність та постійне адаптування до зростаючих викликів. Важливість розуміння та визначення цих термінів у контексті сучасного інформаційного суспільства підкреслюється необхідністю вироблення чітких та уніфікованих тлумачень для ефективного впровадження стратегій кібербезпеки.

Зокрема, з'ясовано, що кібербезпекова політика включає в себе комплекс заходів, спрямованих на запобігання, виявлення та реагування на кіберзагрози з метою забезпечення стабільності та безпеки інформаційних

систем. Визначено, що ця політика має бути гнучкою та адаптивною, охоплюючи не лише технічні аспекти захисту, а й правові, етичні та соціокультурні виміри. Результати аналізу свідчать про необхідність системного та комплексного підходу до формування та реалізації кібербезпекової політики. З вищезазначеного вбачається принципова важливість взаємодії між різними суб'єктами, включаючи державні і недержавні організації, бізнес та академічне середовище для успішної реалізації стратегій кібербезпеки.

Отже, удосконалення понятійно-категоріального апарату є ключовим етапом для ефективного управління та захисту в інформаційному просторі, що надає змогу пристосовуватися до зростаючих загроз та забезпечувати стійкість кіберпростору в умовах сучасного технологічного розвитку.

3. Дослідження поняття, сутності та ознак кіберзлочинності в міжнародному праві дозволило визначити важливі аспекти цього явища та висвітлити ключові аспекти його правового визначення та регулювання. Однією з визначальних ознак кіберзлочинності є її транскордонний характер, що вказує на необхідність міжнародного співробітництва у боротьбі з цим явищем. Сутність кіберзлочинності полягає в незаконному використанні інформаційно-комунікаційних технологій для скоєння правопорушень, включаючи атаки на комп'ютерні системи та мережі.

Визначено, що існуючі нормативно-правові акти та конвенції в сфері кіберзлочинності потребують подальшої адаптації та розширення, охоплюючи нові виклики та загрози, які виникають у зв'язку з розвитком технологій. Необхідність розроблення єдиної та всебічної системи міжнародного правового регулювання кіберзлочинності стає дедалі більш актуальною. Окрім того, важливо враховувати принципи захисту прав людини та забезпечення пропорційності та ефективності заходів при розробці та впровадженні міжнародних правових механізмів у цій сфері.

Отже, подальший розвиток та удосконалення міжнародного правового регулювання кіберзлочинності є стратегічно важливим завданням для

забезпечення кібербезпеки та правопорядку в глобальному інформаційному середовищі.

4. У сучасному світі існує механізм боротьби з транснаціональною злочинністю, зокрема кіберзлочинами, які скоюються в кіберпросторі. Цей механізм ґрунтується на міжнародно-правових документах, які регулюють відносини у сфері міжнародної злочинності в цифровому середовищі. Ключовими елементами такого правового регулювання є Конвенція ООН проти транснаціональної організованої злочинності 2000 року та Конвенція Ради Європи про кіберзлочинність 2001 року з Додатковим протоколом від 2003 року.

Проте, актуальність виникає у необхідності створення універсальної міжнародної конвенції для протидії кіберзлочинності та загального кодексу принципів поведінки держав у світовому інформаційному просторі. Взаємодія в протидії кіберзлочинності вимагає активного міжнародного співробітництва, взаємодопомоги та підтримки, а також постійного оновлення законів на міждержавному та національному рівнях.

Розробка та гармонізація національного законодавства для протидії кіберзлочинності вимагають встановлення міжнародних стандартів криміналізації кіберзлочинів. Враховуючи глобальний характер кіберпростору, важливим є глобальний підхід до розв'язання завдань у сфері боротьби з міжнародною кіберзлочинністю.

5. Кіберзлочинність є однією з складних проблем, які останнім часом викликають суттєвий інтерес міжнародної спільноти у зв'язку з розвитком інформаційних та комунікаційних технологій. Забезпечення кібербезпеки, дотримання прав людини та захист важливої інформаційної інфраструктури вимагають від держав значних зусиль як на національному, так і на міжнародному рівнях. Пріоритетним завданням світової спільноти є розробка та прийняття універсальної конвенції для протидії кіберзлочинності.

Сучасний світ стоїть перед складними викликами у сфері кіберзлочинності, вимагає комплексних та ефективних заходів для боротьби та попередження цього виду злочинів. Виклики, які стоять перед міжнародним співтовариством у цій сфері, включають неоднозначність правового регулювання, відсутність єдиної угоди та швидко змінювану технологічну картину. Невизначеність в аспектах екстериторіального доступу до даних, проблеми конфіденційності та визначення компетентності в кіберпросторі стають перешкодою для ефективної правової боротьби з кіберзлочинністю.

Потреба у подальшій стандартизації законодавства, сприянні міжнародній співпраці та розробці нових форм міжнародних договорів стає нагальною. Розвиток єдиної конвенції чи кодексу, що регулює кіберзлочинність, має потенціал стати важливим кроком для створення єдиного стандарту правил у цій області. Попри існуючі труднощі, ініціативи щодо створення універсальної конвенції та удосконалення міжнародного співробітництва є перспективними. Забезпечення кібербезпеки та захисту прав людини в цифровому просторі потребує спільних зусиль та визначення чітких правових механізмів.

Таким чином, подолання викликів кіберзлочинності вимагатиме не лише вдосконалення законодавства, але і зміцнення співпраці міжнародного співтовариства для створення ефективної системи захисту в кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрушко П. Використання модельних норм Конвенції Ради Європи «Про кіберзлочинність» та Додаткового протоколу до неї у нормотворчому процесі в Україні: теоретичні проблеми реалізації. Право України: юридичний журнал. Міністерство юстиції України; Конституційний Суд України та ін. Київ. 2007. № 12. С. 64-68.
2. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / За заг. ред. О.М. Бандурки. Харків. 2016. 366 с.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. №2(42). С. 54-62.
4. Бєляков Г.Р. Принципи та правове регулювання діяльності управління боротьби з кіберзлочинністю МВС України. Вісник Харківського національного університету внутрішніх справ: збірник наукових праць. Харків. 2014. № 4 (67). С. 17-25.
5. Біленчук П., Малій М. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи. Юридичний Вісник України. 2019. №39. С.14-15.
6. Болгов В.М., Гадіон Н.М., Гладун О.З.. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. Київ: Національна академія прокуратури України. 2015. 202 с.
7. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ. 2015. 288 с.
8. Буяджи С.А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. Право України. 2017. № 9. С. 245-251.
9. Буяджи С.А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект. Дис. наук. канд. юр. наук за спеціальністю

12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Івано-Франківськ. 2018. 203 с.

10. Буяджи С.А. Тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. Вісник Чернівецького факультету Національного університету «Одеська юридична академія». 2017. № 2. С. 21-32.

11. Васильєв А.А. Особливості кваліфікації кіберзлочинів проти власності. Проблеми правознавства та правоохоронної діяльності. 2016. № 4 (58). С. 136-143.

12. Великий енциклопедичний юридичний словник. НАНУ; Ін-т держави і права ім. В.М. Корецького; Редкол.: Шемшученко Ю.С., Горбатенко В.П., Касяненко Ю.Я., Авер'янов В.Б. та ін. Київ: Юридична думка. 2007. 992 с.

13. Власова Г.П. Проблеми боротьби з кіберзлочинністю. Актуальні питання реформування правової системи України : зб. матеріалів XII Міжнар. наук.-практ. конф. (м. Луцьк, 26-27 черв. 2015 р.). Східноєвроп. нац. ун-т ім. Лесі Українки, Юрид. ф-т; уклад. Л.М. Джурак; редкол.: Коцан І.Я. (голова) та ін. Луцьк: Вежа-Друк. 2015. С. 171-173.

14. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Науковий журнал Право і Безпека. 2021. №4. http://archive.nbuv.gov.ua/portal/soc_gum/pib/ 2011_4/PB–4/PB–4_26.pdf.

15. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL:https://uz.ligazakon.ua/ua/magazine_article /EA013606.

16. Гаращенко Ю.В. Державна політика у сфері кібербезпеки в Україні. Вчені записки ТНУ ім. В.І. Вернандського. Серія: Державне управління. 2019. Том 30 (69). № 1. С.140-145.

17. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. Підприємництво, господарство і право. 2019. № 2. С. 203-207.

18. Гринчак І.В. Кіберзлочинність як злочин міжнародного характеру. Науково-інформаційний вісник. 2015. №12. С.93-98.

19. Грицун О.О. Регулювання питань міжнародної інформаційної безпеки в межах міжнародних організацій. Вісник Запорізького національного університету. Юридичні науки. 2014. №4(1). С. 172-180.

20. Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ: збірник наукових праць. Харківський національний університет внутрішніх справ. Харків. 2014. № 4 (67). С. 65-75.

21. Денькович О. Поняття кіберзлочину у зарубіжній кримінології. Проблеми державотворення і захисту прав людини в Україні: матеріали XXIII звіт. наук.-практ. конф., 7-8 лют. 2017 р. / Львів. нац. ун-т ім. Івана Франка, Юрид. ф-т; редкол.: В.М. Бурдін (голова) та ін. Львів: Львівський національний університет імені Івана Франка. 2017. Ч. 2. С. 130-133.

22. Дерещук Т., Струтинаська Т., Романченко В. Виклики на шляху до ефективної протидії кіберзлочинності в Європейськрму Союзі. Філософія та політологія в контексті сучасної культури. 2022. Т. 14. № 2. С. 110-118.

23. Дзюндзюк В.Б. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.

24. Дзьобань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу. Стратегічні пріоритети. Серія: Філософія. 2017. № 3. С. 163-170.

25. Дзьобань О. П. Темпоральна складова у просторово-часовому континуумі віртуальної реальності. Стратегічні пріоритети. Серія: Філософія. 2018. № 2 (47). С. 118-126.

26. Дика Н. В., Одарченко Р. С. Аналіз вимог до системи безпеки 5G. Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників IV Міжнародної науково-практичної конференції (Закарпатська область, Міжгірський район, село Верхнє Студене,

туристичний комплекс «Едельвейс». 21 – 24 лютого 2018 р.). Київ: Видавництво Європейського університету. 2018. С.32-34.

27. Дика Н. В., Одарченко Р. С., Абакумова А. О. Дослідження вимог до стільникових мереж нового покоління та можливості їх розгортання в Україні. Проблеми інформатизації та управління. 2016. Том 2. № 54. С. 52-59.

28. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. URL: http://goal-int.org/sistema-zabezpechennya-kiberbezpe ki-sutnist-ta-priznachennya.

29. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення: монографія. Херсон: Гельветика. 2017. 548 с.

30. Діордіца І. В. Поняття та зміст кіберзлочинності. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti.

31. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Міжнародний документ від 28.01.2003. Офіційний вісник України 2010 р. № 56.

32. Дубов Д. Кібербезпекова політика в контексті трансформації політики безпеки США за адміністрації Б. Обами. Політичний менеджмент. 2010. №1. С.155-162.

33. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД. 2014. 328 с.

34. Забара І.М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. Часопис Академії адвокатури України. 2012. № 17. С. 1-6.

35. Йона О.О. Світові тенденції боротьби з кіберзлочинністю. Вісник Східноукраїнського національного університету імені Володимира Даля. 2013. № 15(1). С. 59-61.

36. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172-177.

37. Ісмайлов К. Ю. Кіберпростір як сфера глобальних конфронтацій. Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали всеукраїнського науково-практичного семінару (м. Дніпро, 25 листопада 2016 р.). Дніпро: Дніпропетровський державний університет внутрішніх справ. 2016. С. 96-101.

38. Каланча С. Г. Кіберзлочинність: шляхи попередження та протидії. Наше право: науково-практичний журнал. Харк. нац. ун-т внутрішніх справ; Кримінологічна асоціація України. Дрогобич. 2012. № 3. ч.2. С. 213-217.

39. Карпінський М., Ткач Ю., Усов Я., Захищене інформаційне середовище. ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р. Київ: НАУ. С. 45-46. 2019.

40. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Міжнародний документ від 15.11.2000. Офіційний вісник України. 2006 р. № 14. стор. 340.

41. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу. Міжнародний документ від 29.05.2000.URL://zakon3.rada.gov.ua/laws/show/994_238?test=Up9Mf3o6frtCt4d2ZiIViVNw HI4Uks80msh8Ie6.

42. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. Офіційний вісник України. 2007 р. № 65. стор. 107. стаття 2535. код акту 40846/2007.

43. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С. 127-130.

44. Котух Є. Кіберзброя: проблеми та перспективи протидії кіберзлочинності. Зовнішні справи: суспільно-політичний журнал. Київ. 2012. № 4. С. 38-40.

45. Ліпкан В.А., Ліпкан О.С. Національна і міжнародна безпека у визначеннях та поняттях. Вид. 2- доп. і перероб. Київ: Текст. 2008. 400 с.

46. Літвінов М.Ю. Світова та українська практика боротьби з кіберзлочинністю. Право і безпека: науковий журнал. Харк. нац. ун-т внутрішніх справ. Харків. 2014. № 1 (52). С. 85-89.

47. Лук'янчук Р.В. Сучасний формат державного регулювання процесів забезпечення кібернетичної безпеки: досвід європейського союзу. Вісник Київського національного університету імені Тараса Шевченка. Київський національний університет імені Тараса Шевченка. Київ. 2016. Вип. 2 (6). С. 34-38.

48. Луньова О.С. Окремі аспекти правового регулювання розслідування кіберзлочинів в Україні. Актуальні питання розслідування кіберзлочинів. Харків, 2013. С. 106-110.

49. Люта Н.В. Кіберзлочини як сучасна загроза фінансовій безпеці банків та їх клієнтів. Наука: теорія та практика: зб. тез доп. III Всеукр. наук.-практ. заоч. конф., 16-18 жовт. 2014 р. М-во освіти і науки України, Черкас. нац. ун-т ім. Богдана Хмельницького. Черкаси: Чабаненко Ю.А. 2014. С. 247-252.

50. Марущак А.І. Міжнародне співробітництво У боротьбі транснаціональною 3 кіберзлочинністю. Інформація і право. 2018. № 3(26). С. 104-110.

51. Обама представив новий план оборонної стратегії США. URL: https://www.holosameryky.com/a/us-defense-2012-01-05-136732543/246777.html

52. Орлов О.В. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. Теорія та практика державного управління. 2013. Вип. 4. С. 17-23.

53. Платоненко А.В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. Науковий журнал. 2015.

54. Погорецький М. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.

55. Попова Т. В., Ліпкан В.А. Стратегічні комунікації: словник /за заг. ред. д-ра юрид. наук. В. А. Ліпкана. Київ: О. С. Ліпкан. 2016. 416 с.

56. Про Національну безпеку України: Закон України від 21. 06.2018 року № 2469-VIII.

57. Продан Т.В. Протидія кіберзлочинності в Україні. Свобода, безпека та незалежність: правовий вимір: Матеріали XIII Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 24 лютого 2023 р. С. 370-372.

58. Пушкаренко П.І. Кіберзлочинність як новітній феномен тіньової економіки. Проблеми і перспективи розвитку банківської системи України: зб. наук. праць. Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми, 2006. Т. 17. С. 75-82.

59. Резолюція 45/113 Генеральної Асамблеї ООН від 14 грудня 1990 року. URL: http://zakon4.rada.gov.ua/laws/show/995_204.

60. Росинський А. В. Кіберзлочинність як виклик економічній безпеці підприємства в умовах форсованої цифровізації. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/4d24d9dd-2d11-4eca-928e-af25187f8adc/content.

61. Рудник Л. І. Право на доступ до інформації: дис. канд. юрид. наук: 12.00.07. Київ. 2015. 247 с.

62. Рудой К.М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України. Публічне право: науково-практичний юридичний журнал. Всеукр. громадська організація «Майбутнє країни»; Ужгород. нац. ун-т. Київ. 2015. № 3 (19). С. 144-149.

63. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки: збірник наукових праць. МОНУ; КНУ імені Тараса Шевченка; Ін-т конкурентного суспільства. Київ. 2009. Вип. 19. С. 338-342.

64. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Вип. 64. С. 386-391.

65. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Справедливість у юриспруденції: теорія та практика: зб. матеріалів Міжнар. юрид. наук.-практ. конф.: тези наук. доповідей (23 лютого 2016 р.) Відп. за вип. Н.І. Смеречинська. Київ: Актуальна юриспруденція. 2017. С. 54-58.

66. Сироїд Т.Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини. 2014. С. 194–196.

67. Сігова Х.В. Кіберзлочини як загроза для кожного. URL: https://core.ac.uk/reader/84825410.

68. Скулиш Є.Д Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. Інформація і право. 2014. № 1(10). С. 93-100.

69. Скулиш Є.Д. Посилення відповідальності в контексті підвищення ефективності боротьби із кіберзлочинністю. Правова інформатика. 2020. № 4 (40). С. 90–97.

70. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб’єктів запобігання кіберзлочинності. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право. 2018. № 6 (18). С. 154-163.

71. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи: монографія. Одеса: Фенікс. 2020. 404 с.

72. Ткач Ю. Тенденції розвитку сучасного кіберпростору та його захищеності в умовах інформаційного протиборства. Ukrainian Scientific Journal of Information Security.2020.Vol. 26. Is. 2. PP. 74-79.

73. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа:інформаційні технології в соціокультурній сфері. 2018. №1. С. 75–86.

74. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року URL http://base. spinform.ru/show_doc.fwx?rgn=28340.

75. Угода про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації. Міжнародний документ від 01.06.2001. URL http://zakon4.rada.gov.ua/laws/show/997_353.

76. Форос Г.В. Правові основи захисту інформації в кіберпросторі. Правова держава. 2018. № 30. С. 181-186.

77. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. №2(5). С. 162–175.

78. Цимбалюк В.С. Кіберпростір як компонент національної безпеки: політико-правивий аспект. DOI https://doi.org/10.30525/978-9934-26-223-4-163.

79. Чернєй В.В. Роль відомчої освіти та науки в забезпеченні протидії кіберзлочинності в Україні. Науковий вісник Національної академії внутрішніх справ. 2014. № 3. С. 3-15.

80. Шемчук В.В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. Вчені записки ТНУ імені В.І. Вернадського. Серія: Юридичні науки. 2022. № 2. Т. 29 (68). С. 125-130.

81. Шепетько С.А. Міжнародний досвід протидії транснаціональній організованій злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 1. С. 298-306.

82. Яцишин М.Ю. Проблеми та перспективи розвитку міжнародно-правового співробітництва у боротьбі з кіберзлочинністю. Порівняльно-аналітичне право. 2018. №5. С.395-398.

83. Banks W. State Responsibility and Attribution Cy-ber Intrusions After Tallinn 2.0. Texas Law Review. Vol 95 (7). 2017. P. 1487-1513.

84. Brown D. Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. URL: https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.

85. Choi K., Lee C.S. The Present and Future of Cybercrime, Cyberterrorism and Cybersecurity. International journal of Cybersecurity Intelligence and Cybercrime. 2018. P. 1-4.

86. Wessel R.A. Towards EU cybersecurity law: Regulating a new policy field. Research Handbook on International Law and Cyberspace. Cheltenham: E. Elgar. P. 403–425.