МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА НАЦІОНАЛЬНОГО, МІЖНАРОДНОГО ПРАВА
ТА
ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРЗЛОЧИННОСТІ В МІЖНАРОДНОМУ КОНТЕКСТІ: ВИКЛИКИ ТА СТРАТЕГІЇ БОРОТЬБИ

Кваліфікаційна робота (проєкт)

на здобуття ступеня вищої освіти «бакалавр»

Виконала: студентка IV курсу 10-481 група
Спеціальності: 293 Міжнародне право
Освітньо-професійної програми «Міжнародне право»
Страшенко Наталія Сергіївна
Керівник **к.ю.н., доц. Гладенко О.М.**

Рецензент **д.ю.н., доцент Кронівець Т.М.**

Івано-Франківськ – 2024

ЗМІСТ

ВСТУП

Актуальність дослідження теми визначається невпинним розвитком технологій поширенням кіберзлочинності на глобальному рівні. Сучасна інформаційна ера надала злочинцям нові можливості для здійснення атак на комп'ютерні системи, електронні мережі та критичну інфраструктуру, що створює серйозні загрози для безпеки країн та міжнародної стабільності.

Зростання обсягів кіберзлочинності призводить до необхідності ефективного міжнародного співробітництва у сфері правового регулювання. Відсутність стандартизованих та добре адаптованих правових механізмів створює прогалини для уникнення відповідальності злочинцями та ускладнює виявлення та покарання кіберзлочинів. Зокрема, важливо вивчати та розробляти міжнародні правові рамки, спрямовані на попередження, виявлення та припинення кібератак, а також на ефективне покарання винних сторін.

Дослідження цієї теми важливе також через постійне зростання нових технологічних викликів, які викликають ускладнення визначення та класифікації кіберзлочинності. Розуміння та адаптація правових механізмів до сучасних тенденцій у кіберпросторі є ключовим елементом забезпечення безпеки та стабільності на міжнародному рівні. Таким чином, дослідження даної теми відкриває можливості для розробки ефективних стратегій боротьби з кіберзлочинністю та покращення міжнародного співробітництва для забезпечення цифрової безпеки.

Мета і завдання дослідження. Метою даного дослідження є вивчення та аналіз правового регулювання кіберзлочинності в міжнародному контексті з акцентом на визначення викликів, які виникають внаслідок постійного розвитку технологій та їх впливу на безпеку інформаційного простору. Дослідження спрямоване на ідентифікацію прогалин у існуючих міжнародних правових механізмах, які ускладнюють ефективне протидію кіберзлочинності.

Відповідно до поставленої мети можна запропонувати наступні **завдання**:

– Охарактеризувати поняття та ознаки кіберзлочинності згідно міжнародного права;

– Проаналізувати історію розвитку міжнародно-правового регулювання боротьби з кіберзлочинністю;

– Визначити особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму;

– Охарактеризувати напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю;

– Проаналізувати Європейський досвід подолання кіберзлочинності в Україні в умовах сьогодення.

Об'єктом дослідження є суспільні відносини, що виникають у сфері правового регулювання кіберзлочинності в міжнародному контексті: виклики та стратегії боротьби.

Предметом дослідження виступає правове регулювання кіберзлочинності в міжнародному контексті: виклики та стратегії боротьби

Методи дослідження включають теоретичний аналіз та синтез, метод порівняння, графічний та табличний методи, логічний та системний аналізи тощо. У ході написання дипломної роботи також проводиться аналіз поставленого завдання з використанням загальнонаукових методів.

Практичне значення отриманих результатів дослідження виявляється в низці ключових аспектів, що сприяють вдосконаленню сучасних підходів до боротьби з кіберзлочинністю та забезпеченню цифрової безпеки.

Отримані результати визначають можливість вдосконалення міжнародних правових механізмів, спрямованих на протидію кіберзлочинності. Рекомендації та пропозиції, розроблені на основі дослідження, можуть слугувати основою для розробки нових міжнародних конвенцій та угод, спрямованих на уніфікацію правових стандартів у цій області.

Результати дослідження дозволяють сформулювати ефективні стратегії боротьби з кіберзлочинністю, які орієнтовані на міжнародний рівень. Це включає в себе розробку спільних програм технічного співробітництва, обмін даними між країнами та встановлення міжнародних стандартів щодо захисту кіберпростору.

Дослідження може слугувати основою для розробки рекомендацій з вдосконалення внутрішніх правових механізмів кожної країни, спрямованих на протидію кіберзлочинності. Це включає в себе удосконалення законодавства, розробку технічних засобів виявлення та реагування на кіберзлочини, а також підвищення кваліфікації правоохоронних органів та судових структур у цій сфері.

Отже, отримані результати дослідження стають підґрунтям для практичних заходів з удосконалення міжнародного та національного правового регулювання кіберзлочинності, що сприяє покращенню глобальної цифрової безпеки та зменшенню вразливості суспільства перед сучасними кіберзагрозами.

Структура роботи. Робота складається зі змісту, вступу, основної частини (трьох розділів, поділених на підрозділи) загальних висновків, списку використаних джерел, який нараховує 28 найменувань. Робота містить 4 таблиці. Загальний обсяг роботи 37 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ АСПЕКТ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

1.1. Поняття та ознаки кіберзлочинності згідно міжнародного права

З появою нових технологій, удосконаленням Інтранет-провайдінгів, кожна людина все більше занурюється у віртуальне середовище, що означає наступне: чим більше нових можливостей, тим більша ймовірність того, що кожен з нас може зіткнутися з новими проблемами, зокрема, з Інтранет - шахрайством.

Ю.С. Шемшученко визначає Інтернет у світлі теорії права як передусім новий простір людського самовираження; міжнародний простір, що перетинає будь-які межі; децентралізований простір, яким ніякий оператор, жодна держава повністю не володіє та не керує [1, с. 321].

Так, В.І. Акуленко вважає, що поняття «комп'ютерна злочинність» замало охоплення всіх діянь, скоєних з допомогою обчислювальної техніки, світових мереж. Кіберзлочинність, на її думку, - це сукупність злочинів, що скоюють в кіберпросторі або за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж або комп'ютерних мереж даних [1, с. 323].

Враховуючи той факт, що зараз велика кількість інформації: фото, відео, контакти близьких і друзів, геолокація, певні програми з важливими даними, паролі, особисті листування та багато іншого, зберігаються на електронних носіях, кожен власник наражає конфіденційність своїх даних на небезпеку.

Варто врахувати той факт, що власниками інформації, що має вагоме значення, можуть бути не тільки індивіди, а й організації, компанії, країни.

Таким чином, прогрес суспільства у сфері інформаційних технологій, широке впровадження та використання передових технологій збору та обробки інформації є не лише невід'ємною частиною життя кожного суб'єкта

суспільства, а й створюють передумови для можливих протиправних дій щодо інформації, її користувачів, а також інформаційних систем зв'язку , що веде до зниження рівня забезпечення інформаційної безпеки особистості, суспільства та держави загалом.

Говорячи про міждержавний рівень цієї проблеми, необхідно зазначити той факт, що розуміння масштабів злочинності призвело до прийняття Радою Європи Конвенцію про кіберзлочинність, яка дозволила узгодити учасниками кримінально-правові норми, пов'язані зі злочинами в кіберпросторі. Спільні зусилля учасників держав також дозволили забезпеченню швидкого та ефективного режиму міжнародного співробітництва у цій галузі. Також було розроблено процесуальне законодавство, необхідне для розслідування таких злочинів та судового переслідування осіб, які їх вчинили, у тому числі способи збирання доказів, які знаходяться в електронній формі.

Як наголошує О.В. Бігняк, «значення ухвалення Конвенції надзвичайно велике. Цей документ став, по суті, першим міжнародним договором міжнародного рівня, який регулює правові та процедурні аспекти кримінального переслідування за протиправну діяльність у глобальних мережах. Він чітко визначає, у яких напрямах мають докладатися основні зусилля на національному та міжнародному рівнях» [2, с. 71].

Щоб розглянути заходи протидії кіберзлочинність, необхідно розібрати безпосередньо поняття і види кіберзлочинності.

Кіберзлочинність, визнана досить серйозною проблемою всього сучасного світового співтовариства, що завдає суттєвої шкоди як національній, так і світовій економіці, безпеці, може бути виражена в «класичних» діяннях, скоєних у кіберпросторі за допомогою застосування інформаційно-телекомунікаційних технологій, характеризуючись як високим рівнем латентності, так і масштабності, обумовленої скоєнням злочину в будь-якому місці розташування мережевих структур, застосування названих технологій та підключення до мережі Інтернет. Кіберзлочинності властиві

складності розслідування (пошук суб'єкта злочину, відшкодування заподіяної матеріальної шкоди та ін.) [2, с. 73].

У доповіді Ради Європи щодо проблем у сфері кібербезпеки, кіберзлочинності та її класифікації кіберзлочин визначено як суспільно небезпечне діяння, вчинене в інформаційно-телекомунікаційній сфері за допомогою застосування інформаційно-комунікаційних технологій, тобто з допомогою комп'ютерної системи чи мережі, безпосередньо - у названій системі чи мережі, чи проти названих об'єктів. Цей вид діянь відбито як CIA-offences, тобто як суспільно небезпечні посягання, спрямовані як проти приватності (конфіденційності; confidentiality), так і єдності (цілісності; integrity), а також проти відкритості (availability) даних та інформаційних систем [3, с. 13].

У 1991 році Інтерпол внесла вагомий внесок у сферу боротьби з інформаційними (кібер) злочинами, представивши власну систему класифікації, яка детально розглядає різноманітні аспекти цього складного проблемного питання. Запропонована класифікація охоплює широкий спектр кіберзлочинів, серед яких виділяються наступні:

– QA – Несанкціонований доступ та перехоплення: Цей вид кіберзлочину охоплює неправомірний доступ до інформації та її неправомірне перехоплення, що може призвести до серйозних порушень приватності та безпеки.

– QDT – Троянський кінь: Злочин полягає в інтродукції та розповсюдженні програм, які маскуються під корисний софт, але фактично завдають шкоди, зокрема, шляхом надання несанкціонованого доступу до системи.

– QAT – Крадіжка часу (ухилення від плати за користування): Даний тип кіберзлочину включає в себе використання різних методів для ухилення від сплати вартості користування ресурсами, що може створити фінансові втрати та порушити правила економічної взаємодії.

– QDV – Комп’ютерний вірус: Цей кіберзлочин передбачає інтродукцію та поширення вірусів, які можуть завдати шкоди системам та даним, порушуючи їхню цілісність та функціональність.

– QD – Зміна комп’ютерних даних: Кіберзлочин включає в себе неправомірну модифікацію існуючих комп’ютерних даних, що може призвести до серйозних наслідків для систем та користувачів.

– QFC – Шахрайство з банкоматами: Цей тип злочину спрямований на незаконне отримання доступу до банкоматних систем та виведення фінансових коштів без належних авторизацій.

– QF – Комп’ютерне шахрайство: Кіберзлочин охоплює різноманітні обманні дії, які використовуються в мережі з метою отримання несанкціонованого доступу або здійснення інших протиправних вчинків.

– QZ – Інші комп’ютерні злочини: Категорія включає різноманітні комп’ютерні порушення, які не вписуються в попередні категорії, охоплюючи широкий спектр можливих інцидентів.

– QR – Незаконне копіювання: Наведений тип кіберзлочину стосується незаконного копіювання та поширення програм, даних чи контенту, порушуючи авторські права та закони про інтелектуальну власність.

– QFT – Телефонне шахрайство: Даний вид кіберзлочину включає в себе обманні дії, спрямовані на отримання несанкціонованого доступу до телефонних систем або інших телекомунікаційних ресурсів.

– QS – Комп’ютерний саботаж: Злочин передбачає активні дії, спрямовані на систематичне завдання шкоди комп’ютерним системам та інфраструктурі.

– QFF – Комп’ютерна підробка (та інші): Категорія включає різноманітні форми підробки та обману в комп’ютерному середовищі, що можуть призвести до непередбачуваних наслідків [3, с. 13-15].

Вибачається, що наведена комплексна класифікація кіберзлочинів, впроваджена Інтерполом, становить важливий крок у розумінні та боротьбі з цими загрозами для сучасного суспільства. Враховуючи широкий спектр

аспектів, що включаються в цю класифікацію, вона служить ефективним інструментом для розробки стратегій та заходів, спрямованих на протидію та запобігання кіберзлочинам.

Відповідно до Конвенції Ради Європи з питань боротьби з кіберзлочинністю, яка отримала затвердження Верховною Радою України, ідентифіковано чотири основні види кіберзлочинів:

1) Порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем, що включає незаконний доступ, нелегальне перехоплення, втручання у дані, втручання в систему та зловживання пристроями.

2) Комп'ютерні правопорушення, такі як підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами.

3) Правопорушення, пов'язані зі змістом, включаючи порушення, пов'язані з дитячою порнографією.

4) Порушення авторських або суміжних прав [4].

В.П. Дулепа, за характером використання комп'ютерів чи комп'ютерних систем відзначає три види кіберзлочинів: діяння, де комп'ютери є предметами злочинів (викрадення інформації, несанкціонований доступ, знищення чи пошкодження файлів і пристроїв тощо); події, де комп'ютери застосовуються як знаряддя злочину (електронні розкрадання тощо); злочини, де комп'ютери грають роль інтелектуальних засобів (наприклад, розміщення в інтернеті порносайтів) [5, с. 593]. Ю.М. Батурін та С. А. Буяджи виділяють дві групи комп'ютерних злочинів - пов'язані з втручанням у роботу комп'ютерів і комп'ютери, що використовують, як необхідні технічні засоби [6, с. 58].

З наведеного, слід навести класифікаційні ознаки та види сучасних кіберзлочинів у табл.1.1.

Багатогранність способів скоєння Інтранет-злочинів створює велику кількість перешкод для своєчасного запобігання цим злочинним діянням і збільшує час пошуку злочинців. Поширеною проблемою у розкритті кіберзлочинів також є той факт, що місце знаходження підозрюваного чи

обвинуваченого невідоме, проте реальної можливості його участі у кримінальній справі немає. Таким чином, органи влади стикаються з проблемою пошуку та оцінки доказів, оскільки дані злочини в більшості випадків відбуваються без залишення так званих «слідів на місці злочину».

Таблиця 1.1

Класифікаційні ознаки та види сучасних кібезлочинів

<table>
<tr><td colspan="4">Кіберзлочини у сфері використання платіжних систем</td></tr>
<tr><td>Скімінг(шимінг)</td><td>Кеш-трапінг</td><td>кардінг</td><td rowspan="2">несанкціоноване списання коштів із банківських рахунків за допомогою систем дистанційного банківського обслуговування</td></tr>
<tr><td>незаконне копіювання вмісту треків магнітної смуги (чипів) банківських карток</td><td>викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки</td><td>незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем</td></tr>
<tr><td colspan="4">Кіберзлочини у сфері електронної комерції та господарської діяльності</td></tr>
<tr><td colspan="2">фішинг</td><td colspan="2">Онлайн-шахрайство</td></tr>
<tr><td colspan="2">виманювання у користувачів інтернету їхніх логінів і паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування чи обміну валюти</td><td colspan="2">заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв’язку</td></tr>
<tr><td colspan="4">Кіберзлочини у сфері інтелектуальної власності</td></tr>
<tr><td colspan="2">піратство</td><td colspan="2">кардшарінг</td></tr>
<tr><td colspan="2">незаконне розповсюдження інтелектуальної власності в інтернеті</td><td colspan="2">надання незаконного доступу до перегляду супутникового та кабельного TV</td></tr>
<tr><td colspan="4">Кіберзлочини у сфері інформаційної безпеки</td></tr>
<tr><td>соціальна інженерія</td><td>шкідливе програмне забезпечення (англ. “malware”)</td><td>протиправний контент</td><td>рефайлінг</td></tr>
<tr><td>технологія управління людьми в інтернет-просторі</td><td>створення та розповсюдження вірусів і шкідливого програмного забезпечення</td><td>контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства</td><td>незаконна підміна телефонного трафіку</td></tr>
</table>

До проблем розкриття кіберзлочинців варто віднести і транскордонність, що означає велику відстань між жертвою та злочинцем.

Враховуючи технології в сучасному суспільстві, також варто відзначити автоматизованість деяких злочинних діянь, тобто виконання певних дій за допомогою спеціальних обладнання, додатків, які з періодичністю, наприклад, знімають гроші з будь-яких карт чи рахунків. Наведена проблема також зводиться до того, що ускладняються пошуки злочинця і втрачається система доказів стосовно особи, оскільки стає неможливим звести місце скоєння злочину і місце перебування злочинця.

Говорячи про наукову літературу, варто врахувати той факт, що на сьогодні, не дивлячись на активне поширення кіберзлочинів, немає чіткого розуміння психологічних механізмів залучення жертв. Здається, для поінформованості кожної людини у суспільстві необхідно створення більшої кількості наукового матеріалу, а також проведення семінарів, на яких доступною мовою будуть передаватися запобіжні заходи, яких необхідно дотримуватися при використанні інтернету. Необізнаність повною мірою про цей злочин, вважаємо, є основною проблемою, вирішення якої дозволить скоротити кількість кіберзлочинів у суспільстві [7, с. 23-24].

Таким чином, особливості кіберзлочинів є: транскордонність; нестандартність способів вчинення; автоматизація злочинних діянь; анонімність діянь; складність розкриття даного виду злочинів (низький відсоток розкриття); взаємодія різних злочинних угруповань; високі прибутки злочинної діяльності.

1.2. Історія розвитку міжнародно-правового регулювання боротьби з кіберзлочинністю

Виникнення міжнародно-правового регулювання щодо боротьби з кіберзлочинністю має свої корені у феномені, який в історії сучасної науки кримінального права та криміналістики був розглядався як маловідомий. Однак на світовому етапі його розвиток налічує вже понад півстоліття,

зводячи своє походження до епохи початку 1940-х років, коли перші кроки в галузі комп’ютерної техніки викликали експансію кіберзлочинності [8, с. 138].

З самого свого зародження кіберзлочинність стала невід’ємною складовою сучасного кримінального середовища, викликаючи серйозні виклики для правоохоронних органів та правових систем усього світу. В цьому контексті виникає необхідність у впровадженні міжнародних механізмів регулювання для ефективної боротьби з цією новою формою кримінальної діяльності.

З першими проявами кіберзлочинності в 1940-х роках почалася активна дискусія про необхідність створення міжнародних нормативних актів для регулювання цього явища. З часом стало очевидним, що відсутність чіткої міжнародної правової бази у сфері кіберзахисту створює великі ризики для глобальної безпеки [8, с. 138-139].

На початку 21-го століття відбулися ключові події у формуванні міжнародного правового регулювання кіберзлочинності. Однією з най значущіших стало розроблення та прийняття Конвенції Ради Європи Про кіберзлочинність, яка надала конкретний кадр для боротьби з цією проблемою на міжнародному рівні [9, с. 132].

Сучасні виклики, пов'язані з розширенням та еволюцією кіберзлочинності, підкреслюють актуальність міжнародного правового регулювання. Запровадження інноваційних технологій та постійне зростання кількості інтернет-користувачів вимагають постійного вдосконалення правових механізмів та співпраці країн у сфері кібербезпеки.

Міжнародне співробітництво у сфері кіберзахисту стає стратегічно важливим аспектом, а встановлення міжнародних стандартів та норм є необхідністю для створення ефективної системи взаємодії між країнами у протидії кіберзлочинності. Лише через спільні зусилля та стандартизований підхід можна досягти високого рівня безпеки в цифровому просторі, забезпечуючи стійкість та захищеність світової інформаційної інфраструктури.

Історія розвитку міжнародно-правового регулювання боротьби з кіберзлочинністю відображає поступовий перехід від визнання локальності проблеми до необхідності взаємодії всієї міжнародної спільноти у зусиллях по контролю та запобіганню цьому новому типу злочинності [9, с. 132-133].

З появою комп'ютерних мереж у другій половині 20-го століття організована кіберзлочинність стала явищем глобального масштабу, зумовивши необхідність спільної реакції всіх країн та міжнародних організацій. Боротьба з цим явищем переросла в динамічний процес, що визначається швидким розвитком технологій та постійною еволюцією методів кіберзлочинців.

О.Ю. Довженко ідентифікує чотири ключові етапи в історії розвитку міжнародної співпраці у боротьбі з кіберзлочинністю (табл. 1.2) [9, с. 133-134].

Слід відзначити, що в цій динаміці розвитку визначається стратегічна важливість міжнародно-правового регулювання у глобальній боротьбі з кіберзлочинністю. Розширення міжнародного співробітництва та уніфікація правових підходів визначають успіхи у створенні стійких та ефективних механізмів для захисту світового кіберпростору.

У другій половині 1990-х років кіберзлочинність почала демонструвати великий розвиток, визначаючи нові виміри злочинності, які перетворювали це явище з проблеми особистих матеріальних цілей в небезпеку для державної та міжнародної безпеки. Перехід від кіберзлочинів, спрямованих лише на особистий зиск, до тих, що мали стратегічне значення для національної безпеки, визначив новий етап в розвитку цифрової безпеки та викликав необхідність впровадження міжнародних правових механізмів [10, с. 148].

У цей період інтернет-середовище стало не лише платформою для особистих амбіцій, але й сприяло ескалації терористичних загроз, які мали потенційно серйозні наслідки для світової стабільності, що виявилося особливо актуальним у зв'язку із зростанням кількості інтернет-користувачів і залежністю сучасного суспільства від цифрових технологій.

Таблиця 1.2

Ключові етапи в історії розвитку міжнародної співпраці у боротьбі з кіберзлочинністю

№	Етап	Період	Характеристика
1.	Етап зародження	1986 – 1989 рр.	На цьому етапі приймалися перші національні закони, спрямовані на боротьбу з кіберзлочинністю. Світ почав осмислювати потребу у правовому регулюванні цього нового явища, що виявилося викликом для традиційних правових систем.
2.	Етап систематизації	1989 – 2000 рр.	У цей період відбулася систематизація кримінального законодавства окремих країн, спрямована на ефективну боротьбу з кіберзлочинністю. Країни почали адаптувати своє законодавство до викликів цифрової ери.
3.	Етап консолідації європейської спільноти	2000 – 2001 рр.	У цей період визначено та уточнено спільні підходи та стандарти в Європейському союзі щодо боротьби з кіберзлочинністю. Створення єдиної стратегії стало ключовим етапом у формуванні єдиної силової лінії у протидії кіберзагрозам.
4.	Сучасний етап правового регулювання	2001 р. – наші дні	Зараз ми спостерігаємо активний розвиток міжнародно-правових інструментів боротьби з кіберзлочинністю. З'являються міжнародні конвенції, угоди та нормативні акти, адаптовані до сучасних викликів цифрової безпеки.

Одним із перших випадків, що підкреслив новий рівень загрози, стала справа про теракт з використанням Інтернету, розглянута в США у 1998 році. Затримання 12-річного хакера, який спільно з групою інших підлітків планував злам системи контролю дамби, відкрило очі світу на потенційні наслідки такого втручання. В разі успіху атаки могло статися затоплення двох міст із загальною чисельністю населення понад мільйон осіб. Цей випадок, хоч і характеризувався малолітністю та «хуліганським» характером, привернув

увагу до потенційної загрози для життєзабезпечення, яку несла інтернет-кіберзлочинність [10, с. 150].

Розглядаючи цю справу, можна було помітити, що через свою уразливість комп'ютерні системи могли стати ідеальним знаряддям для вчинення терактів, виходячи за межі традиційного кримінального обличчя. Такий інцидент став важливим каталізатором для формування світової свідомості про необхідність регулювання кіберзагроз на міжнародному рівні та введення в дію ефективних механізмів правового захисту.

У другій половині 1990-х років Інтернет перетворився в «другу реальність», яка не лише відображає реальний світ, але й активно впливає на нього. У цьому віртуальному просторі відбувається відтворення всіх значущих подій світу. З'являється явище кібервійни, де першою такою вважається війна НАТО проти Югославії, а також економічна кіберзлочинність, наприклад, комерційні вторгнення в комп'ютерні системи підприємств з метою отримання інформації або припинення їхньої роботи [11, с. 164].

У відповідь на ці виклики починаються перші спроби встановлення міжнародно-правового регулювання боротьби з кіберзлочинністю. У 2000 році була прийнята Конвенція Організації Об’єднаних Націй (ООН) проти транснаціональної організованої злочинності [12], де вживається термін «транснаціональні організовані злочини, які вчиняються з використанням комп’ютерів, телекомунікаційних мереж та інших видів сучасної технології». Аналогічна термінологія використовується в Віденській декларації ООН про злочинність і правосуддя.

У 2001 році був прийнятий ключовий міжнародний документ - Конвенція про кіберзлочинність [4], який встановив визначення кіберзлочинності, термінологію, що застосовується, і накладає обов'язок на держави криміналізувати відповідні дії. Хоча сам термін «кіберзлочинність» не визначається в Конвенції, з її положень випливає, що до цього поняття відносяться, принаймні, незаконний доступ, нелегальне перехоплення комп'ютерних даних, втручання у комп'ютерні дані, втручання у комп'ютерні

системи, зловживання комп'ютерними пристроями, підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами, правопорушення, пов'язані з дитячою порнографією, та порушення авторських і суміжних прав. Прийняття цієї Конвенції визначило початок глобальної всеохоплюючої боротьби проти кіберзлочинності.

Термінологія, використана в чинних міжнародних договорах України, сприяє використанню терміну «кіберзлочини» відмінно від «комп'ютерних злочинів». Зокрема, цей термін використовується в Конвенції Ради Європи про кіберзлочинність, яка набула чинності для України 1 липня 2006 року.

Конвенція передбачає лише обмежену кількість злочинів у сфері комп'ютерної інформації, і більшість випадків кіберзлочинності залишається поза межами статистики. Щоб бути точнішими, в офіційну статистику включається лише 10%, а в кращому випадку 12% від усіх вчинених злочинних дій.

Конгрес ООН, спробувавши визначити сутність кіберзлочинності для попередження злочинності та поводження з правопорушниками, визначив цей термін у своїй резолюції як «будь-який злочин, який може відбуватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі або проти комп'ютерної системи або мережі». Інакше кажучи, кіберзлочинність охоплює будь-які протиправні дії, вчинені в електронному середовищі [13, с. 48]. Отже, можна зробити висновок, що міжнародно-правове регулювання боротьби з кіберзлочинністю перебуває в процесі розвитку. Між державами існує консенсус щодо необхідності подальшої роботи в цьому напрямку, який втілюється у прийнятті ряду основоположних документів. У той же час залишається невирішеними деякі ключові питання, зокрема, навіть термінологічні аспекти. Тому можна очікувати появу нових міжнародних документів, які будуть розроблятися на основі існуючих теоретичних основ.

РОЗДІЛ 2. МІЖНАРОДНО-ПРАВОВИЙ МЕХАНІЗМ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

2.1. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму

Кіберзлочинність сьогодні стала однією з найбільш поширених та виразних форм транснаціональної злочинності. Спектр складних кіберзагроз, що постійно еволюціонують, створює нові виклики для правоохоронних органів по всьому світу. З виникненням цього нового виміру злочинності виникає необхідність використання нових підходів та інновацій для боротьби з кіберзлочинністю.

О. Курбан визначає, що кіберзлочинність не знає кордонів і надає транснаціональним злочинцям можливість діяти без обмежень, використовуючи нові технології та інформаційні ресурси. Великі обсяги даних, які обробляються у мережі, стають об'єктом інтересу для кіберзлочинців, які активно використовують їх для своїх злочинних метою. Це ставить перед правоохоронними органами великі виклики щодо забезпечення кібербезпеки та захисту інформації [14, с. 22].

Сучасна кіберзлочинність також вимагає від правоохоронних органів не лише спеціалізованої технічної експертизи, але й співпраці та обміну інформацією на міжнародному рівні. Саме в цьому контексті важливою стає ініціатива Інтерполу, який створив дві ефективні платформи для боротьби з кіберзлочинністю.

Перша з них - Cybercrime Knowledge Exchange workspace (CKE) - це робочий простір, створений для обміну знаннями та інформацією про кіберзлочинність. Цей простір не лише обробляє загальну інформацію, а й відкриває її для широкого загалу користувачів. Такий відкритий підхід дозволяє створити спільноту експертів, яка може обмінюватися досвідом та

взаємодіяти для більш ефективного вирішення проблем, пов'язаних із кіберзлочинністю.

Друга платформа - Cybercrime Collaborative Platform (CCP) - є спеціальною платформою для спільної роботи в сфері кіберзлочинності. Вона включає в себе операції для підтримки правоохоронних дій і заходів, доступ до яких обмежений. Це надає можливість обмінюватися конфіденційною інформацією та координувати спільні операції для виявлення та припинення кіберзлочинних дій [14, с. 23-24].

В цілому, ініціативи Інтерполу є важливим кроком у напрямку створення єдиної та потужної системи боротьби з кіберзлочинністю. Правоохоронні органи та органи безпеки повинні продовжувати активно співпрацювати, ділитися інформацією та знаннями, щоб забезпечити ефективну відповідь на загрози, які створює цей швидкозмінюваний та складний вимір кіберзлочинності.

Крім того, слід відзначити зв'язок між кіберзлочинністю і пандемією COVID-19. У зв'язку з глобальною соціальною ізоляцією та закриттям кордонів більшість людей у світі перейшла на дистанційну форму праці та освіти, що призвело до зростання онлайн комунікацій як у приватному, так і в державному секторі.

Паралельно з традиційними формами кіберзлочинності, передові цілеспрямовані загрози (APT - Advanced Persistent Threats) продовжують еволюцію та використовуватися для отримання вигоди з ситуації, пов'язаної з пандемією COVID-19. Головною метою APT-атак є напад на критичні об'єкти інфраструктури, включаючи лікарні та лабораторії, де розробляють вакцини. У цьому контексті застосовуються шкідливі програми, програми-вимагачі та DDoS-атаки. Мотивацією для таких атак є не лише фінансовий виграш, але й можливість отримання доступу до особистих даних та іншої конфіденційної інформації, яка представляє велику цінність, таку як оперативні та/або розвідувальні дані. Проте деякі передові країни мають дієву систему протидії кіберзлочинності, які слід навести у таблиці 2.1 [15, с. 118-120].

Таблиця 2.1

Особливості забезпечення кібербезпеки у країнах світу

Країна	**Участь у Конвенції про кібербезпеку**	**Розробка Конвенції ООН «Про забезпечення міжнародної інформаційної безпеки»**	**Основні організації в області кібербезпеки**
Великобританія	+	-	Група безпеки електронної комунікації при Центрі правового зв'язку при МЗС; підрозділ Міністерства оборони щодо захисту від віртуальних загроз
Індія	+	-	Аналітичний і дослідницький відділи зовнішньої розвідки і розвідувальне бюро внутрішньої розвідки
Китай	-	+	Реалізація програми захисту від несанкціонованого підключення до комп'ютера
США	+	-	Центр національної кібербезпеки; Об'єднане кібернетичне командування Збройних сил США
Німеччина	+	-	Спеціальна група при МВС ФРН
Україна	+	-	Департамент кіберполіції при Національній поліції України

Боротьбу з кіберзлочинами проводять не лише окремі країни, а й міжнародні блоки, зокрема, НАТО. За останні роки важливість цієї проблеми отримала відображення у керівних документах блоку. У стратегічній концепції НАТО вперше зазначено кіберпростір як нову сферу військової діяльності альянсу [16, с. 574].

У контексті боротьби з транскордонними злочинами, до яких належить значна частина кіберзлочинів, основна роль відводиться державам. Лише завдяки добре скоординованій діяльності правоохоронних органів різних країн можна зменшити кількість правопорушень у цій сфері.

Міжнародне співробітництво здійснюється за різними напрямками і передбачає створення нормативних актів та розробку спільних рекомендацій,

а також впровадження ефективних моделей організаційної взаємодії між країнами. Потрібно враховувати, що традиційні механізми міжнародного співробітництва, такі як запити та взаємодопомога, що застосовувалися раніше, стають неефективними в епоху, коли злочини можуть відбуватися з будь-якої точки світу зі швидкістю світла [16, с. 574-575].

Правове регулювання справ у сфері боротьби з кіберзлочинами є основою системи протидії цій проблемі. Ускладнює вироблення міжнародних актів аналізована ситуація, оскільки "існуючі закони важко застосовувати, коли йдеться про атаки, що не піддаються локалізації, у планетарних масштабах, докази яких розкидані і віртуальні".

Міжнародна спільнота вже прийняла ряд актів, які мають значення для боротьби з кіберзлочинами, з особливим наголосом на регіональних актах, оскільки узагальнений світовий документ у цей час є важким створити. Проте, важливо відзначити спроби країн розповсюджувати норми глобальних міжнародних договорів на боротьбу з кіберзлочинами або укладати нові договори.

Важливо відзначити, що більшість спеціалізованих законів з боротьби з кіберзлочинами належать до актів Європейського союзу, який має одну з найрозвиненіших у світі систем забезпечення інформаційної безпеки. Наприклад, під час Тамперської наради Європейської ради у жовтні 1999 року було вирішено включити злочини в галузі високих технологій (high-tech crime) серед злочинів, щодо яких потрібно розробити загальний європейський підхід до криміналізації та санкцій. В 2001 році Європейська комісія оприлюднила спеціальне повідомлення з назвою «Створення безпечного інформаційного суспільства через підвищення захищеності інформаційної інфраструктури та боротьби зі злочинами з використанням комп'ютерних засобів». У цьому повідомленні були висловлені пропозиції правового та організаційного характеру стосовно протидії кіберзлочинності в Європейському союзі [16, с. 577].

Як для Європейського Союзу, так і для всієї світової спільноти ключове значення має Конвенція про кіберзлочинність, яка регулює глобальні заходи по боротьбі з кіберзлочинністю і була прийнята Радою Європи в 2001 році [17, с. 113].

Важливо відзначити, що взаємодія держав у сфері боротьби з кіберзлочинами вимагає узагальнення правових норм різних держав при регламентації дій сторін у процесі використання коштів у боротьбі з кіберзлочинами. Зокрема, Центром передового досвіду НАТО в галузі комп'ютерної безпеки випущено збірку рекомендацій «Таллінське керівництво із застосування міжнародного права в кібервійні». Основними завданнями передбачається «адаптація існуючих правових норм щодо збройних конфліктів під специфіку ворожої діяльності у віртуальному просторі» та спроба розробити визначення основних понять у сфері комп'ютерної безпеки[17, с. 113-114].

Другою формою співробітництва держав у боротьбі з кіберзлочинами є створення спеціалізованих органів. Оскільки інформаційна безпека держави пов'язана з її суверенітетом, то створення єдиного органу, який би координував взаємодію держав щодо боротьби з кіберзлочинами, важко, проте створюються допоміжні органи, які керуються єдиними стандартами діяльності, що узагальнюють практику різних країн з питань боротьби з кіберзлочинами.

Велике значення у взаємодії держав-учасниць Європейського союзу має діяльність Європолу та Євроюсту, які беруть «безпосередню участь у боротьбі з кіберзлочинністю на просторі Європейського союзу». Крім зазначених органів, які мають юрисдикційну компетенцію в даній сфері, Європейським союзом створюються і допоміжні органи. Так, 18 січня 2013 р. у Гаазі офіційно відкрито Європейський центр боротьби з кіберзлочинністю. Цілями його створення є збирання та обробка даних щодо кіберзлочинів, проведення експертних оцінок інтернет-загроз, розробка та впровадження передових методів профілактики та розслідування кіберзлочинів, підготовка нових

кадрів, надання допомоги правоохоронним та судовим органам, а також координація спільних дій зацікавлених сторін, спрямованих на підвищення рівня безпеки у європейському кіберпросторі [17, с. 114-115].

Військова взаємодія держав також потребує вирішення питання щодо їхньої співпраці у сфері організаційної підтримки боротьби з кіберзлочинністю. Так, у 2008 р. «за ініціативою Естонії в Таллінні було створено центр передового досвіду НАТО, на даний час він є науково-дослідним та навчальним закладом альянсу, який займається розробкою ключових напрямів розвитку коаліційних можливостей щодо дій у кіберпросторі» [18, с. 75].

Створення даного центру не було єдиним напрямком роботи з організації боротьби з кіберзлочинами в Альянсі: у 2013 р. було завершено розгортання єдиної системи НАТО з реагування на комп'ютерні загрози, що включає два центри реагування на загрози в кіберпросторі (у Брюсселі та Монсі). Крім цього, робляться кроки з перевірки ефективності вже створеної системи відображення кібератак, наприклад, щорічно проводяться навчання «Кіберкоаліція», «Захисний шар» [18, с. 75-76].

Іншими словами, сучасною тенденцією міжнародної протидії кіберзлочинності є розширення сфери взаємодії держав. Реальністю стає оперативна співпраця правоохоронних органів у боротьбі з кіберзлочинами (Інтерпол, Європол, Євроюст), створення та використання єдиної бази даних про кіберзлочинців, про скоєні та заплановані кіберзлочини (насамперед працюючу в режимі 24/7).

2.2. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю

Збільшення у геометричній прогресії кіберзагроз свідчить про необхідність негайного реагування та впровадження комплексних заходів для забезпечення кібербезпеки на всіх рівнях. Сучасне суспільство стає все більше

залежним від інформаційних технологій, що робить його вразливим перед небезпекою кібератак та кіберзлочинності.

Однією з ключових стратегій вирішення цього завдання є постійне вдосконалення технічних та організаційних аспектів кібербезпеки. Розробка та впровадження нових технологій, які здатні вчасно виявляти та ліквідовувати кіберзагрози, стає важливим завданням для спільноти кіберекспертів. Зокрема, розвиток штучного інтелекту, машинного навчання та аналізу великих даних може значно підвищити ефективність систем кіберзахисту [19, с. 181].

Паралельно з технічними заходами, не менш важливою є роль організаційних стратегій. Сприяння культурі кібербезпеки в усіх сферах суспільства та освіта громадян стають пріоритетом. Створення свідомого підходу до безпеки в інтернеті серед користувачів, підвищення кваліфікації фахівців з кібербезпеки та впровадження етичних стандартів в області кіберпростору є критичними компонентами ефективної стратегії.

Міжнародна співпраця також грає важливу роль у протидії кіберзагрозам. Створення міжнародних стандартів кібербезпеки та обмін інформацією між країнами допомагає у створенні єдиної фронтової лінії протидії кіберзлочинності. Ефективна координація та об'єднання зусиль дозволяють створити стійкі міжнародні механізми, які в злагодженій дії можуть виявляти та ліквідовувати кіберзагрози на різних рівнях [19, с. 181-182].

Загалом, збільшення у геометричній прогресії кіберзагроз вимагає комплексного та взаємодіючого підходу. Лише шляхом поєднання технічних і організаційних стратегій, а також міжнародної співпраці можна забезпечити стійку та ефективну кібербезпеку в умовах постійно зростаючої кількості кіберзагроз.

Важливо відзначити, що ефективність розслідувань та арештів кіберзлочинців позначається на результативному рівні, коли ці дії виконуються одночасно та взаємокоординовано в різних країнах. Наприклад, у 2016 році в ході операції, яка об'єднала правоохоронців 30 країн для

припинення діяльності кібермережі "Avalanche", за підтримки Центру боротьби з кіберзлочинністю Європолу (EC3) та Об’єднаної групи боротьби з кіберзлочинністю (J-CAT), а також Євроюсту та Європейської банківської федерації (EBF), було арештовано 178 осіб-співучасників, включаючи організаторів українського походження [20, с. 142].

Останніми роками значно зросла участь українських правоохоронців у подібних операціях. Наприклад, у 2020 році кіберполіція провела 10 міжнародних поліцейських операцій, розкриваючи діяльність «хакерських» угруповань, які завдали збитків країнам ЄС, Великобританії та США на понад $300 млн [21, с. 225].

Згодом, у ході досудового розслідування кіберзлочинів, особливо тих, що доводяться в іншій юрисдикції, виникають виклики у отриманні, зберіганні та оперативному аналізі доказів. Також важливо відзначити, що Україною ще не були імплементовані такі статті Конвенції про кіберзлочинність, як: ст. 16 – «Термінове збереження комп’ютерних даних, які зберігаються» та ст. 17 – «Термінове збереження і часткове розкриття даних про рух інформації» [21, с. 225-226].

У грудні 2019 року Генеральна Асамблея ООН прийняла резолюцію 74/247, відзначивши важливість створення Спеціального міжурядового Комітету експертів відкритого типу. Цей комітет, що об'єднує представників усіх регіонів, має за мету розробку всеосяжної міжнародної Конвенції про протидію використанню інформаційно-комунікаційних технологій у кримінальних цілях. Ініціатива передбачає врахування існуючих міжнародних документів та зусиль на національному, регіональному та міжнародному рівнях у боротьбі з використанням інформаційно-комунікаційних технологій для здійснення кримінальних дій.

26 травня 2021 року Генеральна Асамблея ООН ухвалила Резолюцію No75/282 «Протидія використанню інформаційно-комунікаційних технологій у кримінальних цілях». Серед інших аспектів, в резолюції закріплено, що Спеціальний комітет проведе щонайменше шість сесій тривалістю в 10 днів

кожна, розпочавши останню сесію в Нью-Йорку в січні 2022 року, щоб представити проєкт Конвенції на сімдесят восьмій сесії Генеральної Асамблеї [20, с. 145-146].

В рамках національного відгуку на загрози в кіберпросторі, Україна затвердила нову Стратегію кібербезпеки у серпні 2021 року за Указом президента № 447/21. Документ визначає ключові виклики та загрози для країни, такі як активне використання кіберзасобів у міжнародній конкуренції, мілітаризація кіберпростору та розвиток кіберзброї. Особлива увага приділяється нарощенню арсеналу кіберзброї державою-агресором, а також використанню кібератак для виведення з ладу об'єктів критичної інформаційної інфраструктури [22].

Додатково, стратегія висвітлює проблему кіберзлочинності, що може призводити до серйозних матеріальних втрат та використання кіберпростору для вчинення злочинів проти основ національної безпеки України.

Стратегія активно визначає ключову мету «Прагматичне міжнародне співробітництво» для ефективної протидії кіберзлочинності. Україна виявляє намір розвивати відносини з міжнародними партнерами, спрямовані як на збільшення взаємної довіри для спільної відповіді на кібератаки та подолання кризових ситуацій у кібербезпеці, так і на практичну співпрацю. Це включає обмін інформацією про кібератаки та кіберінциденти, спільні кібероперації та розслідування міжнародних кіберзлочинів, а також регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками [21, с. 227-228].

Україна має намір приєднатися до діалогу в межах міжнародних організацій для спільного визначення норм поведінки в кіберпросторі та вдосконалення відповідної нормативно-правової бази. З метою систематичного обміну інформацією про деструктивну діяльність в кіберпросторі з міжнародними партнерами, такими як США, країни-члени ЄС та НАТО, планується створення платформи для такого обміну.

Додатково, у Стратегії чітко визначено необхідність залучення України до перегляду Другого додаткового протоколу до Конвенції про

кіберзлочинність. Це передбачає розроблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших країнах. Зазначається, зокрема, на необхідності розширення, через діалог з міжнародними партнерами, доступу правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю та до телекомунікаційної системи Інтерполу I-24/7 [23, с. 145].

Отже, у Стратегії чітко визначаються шляхи зміцнення міжнародного співробітництва в сфері боротьби з кіберзлочинністю. Проте, успішне виконання визначеної роботи значною мірою залежить від якісного планування конкретних заходів та їх вчасного виконання, що не завжди було враховано при реалізації Стратегії кібербезпеки України 2016 – 2020 років.

Водночас, розглядаючи необхідність підвищення та ефективності співпраці між країнами та приватним сектором у сфері збору електронних даних та інших форм збору електронних доказів злочинів, важливо дотримуватися принципів верховенства права та демократичних норм, які визначені європейськими стандартами. Іншими словами, необхідно створити умови для вільного, відкритого та безпечного кіберпростору, уникаючи тоталітарного ведення стеження та безпідставного блокування користувачів. По суті, знаходження оптимального балансу в цих напрямках виявляється завданням з високим рівнем складності в практичному втіленні.

2.3 Європейський досвід подолання кіберзлочинності в Україні в умовах сьогодення

У сучасному контексті, успіхи країн у внутрішній та зовнішній політиці визначаються не лише їхньою військовою та економічною потужністю, але також вдалістю у встановленні реального контролю над внутрішніми інформаційно-культурними процесами. Невдачі в галузі інформаційних технологій стають серйозною глобальною загрозою безпеки, оскільки вони відкривають можливості для використання інтелектуального потенціалу інших країн у власних цілях, для поширення їхніх ідеологічних цінностей, культури, мови та реалізації, що уповільнює духовний та культурний розвиток інших націй. З метою досягнення своїх політичних цілей держави все більше вдаються до використання методів інформаційної війни.

Висока активність Росії в кіберпросторі представляє головний виклик та загрозу для кібербезпеки України. Російська федерація використовує цей простір для нових можливостей, включаючи розвідувально-підривну діяльність проти України, спеціальні операції з прихованим доступом до кібермереж органів державного управління та критичної інфраструктури. Мета полягає в установленні контролю з метою отримання вигоди та захисту своїх інтересів у сферах інформаційної, військової, політичної, фінансово-економічної та енергетичної. Росія вже розробила кіберзброю для нейтралізації та виведення з ладу об'єктів критичної інфраструктури противника, щоб підвищити ефективність майбутніх атак або максимально послабити їхню здатність до протистояння. Однак таку кіберзброю важко стримати [24, с. 531].

Після початку воєнної агресії росії проти України, компанії, що спеціалізуються на кібербезпеці, зафіксували збільшення кількості кібератак на інформаційні системи країни. Зазвичай ці атаки спрямовані на конфіденційне викрадення важливої інформації, ймовірно, з метою надання росії стратегічної переваги на полі бою. Жертвами російських кібератак стали державні установи України, країни ЄС, США, міністерства оборони,

міжнародні та регіональні оборонні та політичні організації, аналітичні центри, ЗМІ та дисиденти.

ІТ-фахівці вчиняють інформаційні втручання: за даними Google, навіть протягом січня-квітня 2022 року кібератаки на український уряд, військові структури та ІТ-ресурси критичної інфраструктури виявилися більш руйнівними, ніж за попередні вісім років. Важливо відзначити, що пік хакерської активності спостерігався на початку повномасштабного вторгнення росії в Україну.

Ці російські кібероперації спрямовані на три основні завдання:

- Послабити функціонування українського уряду.

- Зупиняти міжнародну підтримку для українського уряду.

- Підтримувати військове вторгнення Росії на територію України [24, с. 531-532].

У наступній таблиці вказано, які види кібератак існують на сучасний момент і на які сфери спрямовані найбільше кількість цих атак.

Таблиця 3.1

Галузі, які зазнають найбільших кібератак з початку вторгнення рф

Галузі кібератак рф на Україну	Відсоток %
Держоргани	27
ІТ-галузь	10
Медіа	9
Енергетика	8
Транспортна галузь	7
Телекомунікації	7
Фінанси	5
Інші	27

З початком російсько-української війни з'явилися антиукраїнські активістські групи, які ідентифікували себе як «Кіберберкут» та проукраїнську «Майдан Кіберсотня», «Анонімі» з російською чи українською «пропискою».

Незважаючи на труднощі в визначенні ступеня співпраці хакерських груп з державними органами, можна стверджувати, що на території росії діють проросійські хакерські групи, які проводять свою діяльність на користь Кремлівського режиму [25, с. 224].

Можна вважати, що з початку російсько-українського конфлікту дослідники кібербезпеки поліпшили свою здатність виявляти, відстежувати та захищати від російських хакерських груп. Одним із можливих пояснень є те, що зі зростанням конфлікту російські хакери не встигають своєчасно оновлювати та вдосконалювати свою тактику, технології та методи роботи.

23 лютого 2022 року, за один день до масованого вторгнення Росії в Україну, була зафіксована кібератака на державні ресурси та банки [3]. О 16:00 розпочалася нова хвиля кібератак, піддавши атакам сайти Верховної Ради, Кабінету міністрів України та МЗС. Міністерство освіти і науки призупинило доступ до свого сайту для запобігання кібератакам. За словами міністра цифрової трансформації Федорова, портал і сайт застосунку «Дія» успішно протистояли атаці [25, с. 224-225]. Згодом виявилось, що також були взяті під контроль сайти СБУ, Міністерства стратегічних галузей промисловості, інфраструктури та агрополітики.

Уночі та вранці 24 лютого 2022 року під час російської атаки на Україну сайт Київської ОДА зазнав хакерської атаки, при цьому деякі ресурси були відключені для захисту інформації. На сайтах i.ua та meta.ua Держспецзв'язку виявила масові розсилки з фішинговими викликаннями на особисті адреси українських військовослужбовців та пов'язаних осіб. Зловмисники використовували протоколи IMAP для компрометації адрес електронної пошти і завантаження електронних листів. За даними агентства, за цим стоять білоруські хакери з групи UNC1151, яка діє в Мінську та включає офіцерів Міноборони Республіки Білорусь [25, с. 225].

Як вже було наведено у попередніх розділах, Україна, відповідно до укладених нею міжнародних угод, співпрацює з іноземними державами у

галузі кібербезпеки, включаючи їх збройні сили, правоохоронні органи та спецслужби, переважно з членами НАТО та ЄС [26].

Інформація щодо забезпечення кібербезпеки, протидії міжнародному кіберзлочинству та кібертероризму передається Україною іноземним державам на основі міжнародних договорів. Ця форма взаємодії охоплює широкий спектр нормативних, методичних, практичних, науково-освітніх питань, організацію актуальних міжнародних семінарів і конференцій, а також надання методичної та практичної допомоги іноземним партнерам. Робочі відносини з провідними фахівцями у галузі кібербезпеки включають налаштування, вивчення та впровадження кращих практик, що вже має позитивний вплив на країну [27, с. 44].

Взаємодія між євроатлантичним і євразійським просторами у сфері кібербезпеки стає ключовою у створенні загальних безпекових інститутів, таких як ООН, ОБСЄ, НАТО, ЄС та РЄ [27, с. 44-45]. Ці організації працюють разом з метою охоплення різноманітних питань безпеки та уникнення дублювання функцій. ООН відіграє особливу роль у вирішенні питань міжнародного співробітництва у сфері боротьби з кіберзлочинністю та постійно обговорює питання запобігання та протидії комп'ютерним злочинам [28, с. 581-582].

Співпраця з НАТО в рамках конструктивного партнерства, спрямованого на високі стандарти протидії сучасним викликам і загрозам, сприяє досягненню передових стандартів обороноздатності України. У контексті розвитку міжнародного співробітництва в сфері кібербезпеки важливим є партнерство з НАТО, що є необхідною складовою євроінтеграційного курсу. Партнерство супроводжується необхідними реформами у секторах оборони та безпеки, а також внутрішніми змінами. Розроблені в такому форматі навчання є підготовкою до щорічного затвердження національної програми співпраці Україна-НАТО на державному рівні [27, с. 46].

ВИСНОВКИ

За результатами проведеного дослідження при написанні дипломної роботи можна дійти наступних висновків.

1. У ході проведеного дослідження теоретико-правових аспектів міжнародно-правового регулювання боротьби з кіберзлочинністю було виявлено ряд ключових висновків. Перш за все, визначено, що термін «кіберзлочинність» не має чіткого нормативно-правового визначення, що створює деяку неоднозначність у розумінні цього явища на рівні міжнародного співтовариства.

Дослідження вказало на те, що термін «кіберзлочинність» часто використовується як синонім до «комп'ютерної злочинності», проте він має ширший характер. Це свідчить про необхідність уточнення та стандартизації термінології для уникнення непорозумінь та створення єдиної бази для правового регулювання в цій сфері.

Крім того, дослідження вказало на те, що кіберзлочинність не обмежується лише комп'ютерними мережами, але охоплює також телекомунікаційні, банківські та інші сфери.

Вирішення проблеми кіберзлочинності вимагає активного співробітництва між державами та розробки нових, спеціалізованих міжнародних нормативно-правових актів. Такий підхід дозволить ефективно протистояти викликам, які виникають у зв'язку з постійним розвитком технологій та зростанням кількості кіберзлочинів, забезпечуючи безпеку та захищеність інформаційних систем на міжнародному рівні.

2. Міжнародне співробітництво відіграє важливу роль у протистоянні правовому розриву, який виникає між динамічним розвитком інформаційних технологій і законодавчою реакцією на сучасні кіберзагрози. Метою міжнародного співробітництва є зміцнення взаємної довіри в області кібербезпеки, розробка спільних стратегій протидії кіберзагрозам, посилення

зусиль у розслідуванні та запобіганні кіберзлочинам, уникнення використання кіберпростору в протиправних цілях.

Крім того, міжнародне співробітництво спрямоване на виконання Україною зобов'язань за міжнародними договорами в галузі співробітництва у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами та спеціальними службами, а також міжнародними організаціями. До інших аспектів такого співробітництва входить надання міжнародної технічної допомоги.

Навіть при мирному використанні та повному роззброєнні міжнародної спільноти у кіберпросторі існує конфлікт та протистояння між групами держав, такими як США, російська федерація і Китай, які прагнуть встановити свою домінувальну позицію та лідерство в цій конкурентній арені, де кожен намагає продемонструвати свою силу та першість. З урахуванням вищевказаного можна стверджувати, що міжнародне співробітництво у сфері кібербезпеки переважно здійснюється через організаційно-правові форми та відіграє важливу роль для забезпечення національної безпеки України.

3. В умовах війни, де кібербезпека є невід'ємною частиною національної безпеки, Україна намагається використовувати європейський досвід у подоланні кіберзлочинності. Активна співпраця з НАТО та ЄС дозволяє країні утримуватися на передовому рівні в цій сфері.

Україна, дотримуючись міжнародних стандартів та договорів, встановлює ефективні партнерські відносини з іншими країнами та організаціями, спрямовані на подолання кіберзлочинності. Співпраця з НАТО не лише сприяє вирішенню конкретних викликів, але й допомагає Україні досягати провідних стандартів у сфері обороноздатності.

Партнерство із Європейським Союзом є необхідним компонентом євроінтеграційного курсу. Спільна робота з ЄС передбачає не лише обмін досвідом, але і впровадження необхідних реформ у секторах оборони та безпеки. Результатом цієї взаємодії є підготовка та вдосконалення

національних програм співпраці, що відображають найкращі практики та інноваційні підходи.

Значущість співпраці в сфері кібербезпеки визначається не лише обміном технічними засобами, а й спільними зусиллями у розробці та впровадженні стратегій, що враховують найактуальніші виклики. Комплексне підходить до навчання та консультації, проведення міжнародних заходів, сприяє вивченню та впровадженню передових методик кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Енциклопедія міжнародного права : у 3 т. / редкол.: Ю.С. Шемшученко, В.Н. Денисов, В.І. Акуленко та ін. Київ : Академперіодика, 2017. Т. 2: Е–Л. 928 с. Дулепа В.П.
2. Бігняк О.В., Грушко М.В., Мануїлова К.В. Теорія міжнародного права : навчально-методичний посібник / за ред. завідувача кафедри міжнародного та європейського права О.В. Бігняка. Херсон : Видавництво «Гельветика», 2020. 224 с.
3. Летичевський, О. О. Сучасні наукові проблеми кібербезпеки. *Вісник НАН України*. 2023. № 2. С. 12-20.
4. Конвенція про кіберзлочинність. Конвенція від 23.11.2001. № 994_575. *Рада Європи*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
5. Дулепа В.П. Кримінологічна характеристика кіберзлочинності. *Юридичний науковий електронний журнал*. 2021. № 11. С. 592–595.
6. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект. Дис...канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.
7. Любавіна В. Сутність кіберзлочинності та способи боротьби. *Науковий журнал «молодий вчений». Юридичні науки*. 2022. №8(108). С. 22-25;
8. Войціховський, А. В. Міжнародне право : підручник; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 544 с.
9. Довженко О.Ю. Становлення міжнародно-правового регулювання боротьби з кіберзлочинністю. Конгрес міжнародного та європейського права : матеріали Міжнар. наук.-практ. конф. (Одеса, 19 квіт. 2019 р.). МОН України, Нац ун-т «Одес. юрид. акад.». Одеса : Фенікс, 2019. С. 131-135.
10. Legan I.M., Bondarenko K.S. Features of the free legal aid system in Ukraine and the European Union countries. *Держава та регіони*. Серія: ПРАВО. 2020. № 3(69). С. 148–151.

11. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.
12. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Конвенція від 15.11.2000. № 995_789. *Організація Об'єднаних Націй(ООН)*. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text
13. Федонюк С.В. Міжнародні аспекти безпеки кіберпростору : монографія / С. В. Федонюк. Луцьк : Вежа-Друк, 2022. 176 с.
14. Курбан О. Проблема критичності мислення при споживанні медіаконтенту в умовах інформаційної війни. *Синопсис: текст, контент, медіа*. 2022. No28 (1). С. 21–27.
15. Леган І.М. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2021 № 50. С. 118-121.
16. Ковалів С.В., Єсімов С.С. Механізм співробітництва держав щодо протидії злочинам у сфері інформаційних технологій. *Електронне наукове видання «Аналітично-порівняльне правознавство». Розділ XI. Міжнародне право*. 2023. № 3. С. 573-578;
17. Мирна Н.В., Білоконь М. В. Європейська інтеграція та протидія гібридним Загрозам: виклики та перспективи. *Теорія та практика державного управління*. 2023. №1 (76). С. 107-122;
18. Костенко, В. О. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті Європейської інтеграції. *Публічне управління та адміністрування в Україні*. 2023. № 33. С. 74-77.
19. Клименко О.А., Гуцалюк М.В. Кримінальний опортунізм кіберзлочинності як загроза національній безпеці України. *Юридичний вісник "Повітряне і космічне право"*. 2021. Т. 1. № 58. С. 177-184.

20. Гуцялюк М.В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. *Інформація і право*. 2021. № 4(39). С. 141-147;
21. Довгань. В.І., Коцман І.І. Основні аспекти державної політики забезпечення протитідії кіберзлочинності в Україні. *Актуальні питання у сучасній науці*. 2023. № 3(9). С. 220-229;
22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26.08.2021. № 447/2021. *Президент України*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12
23. Мігалатюк В. В. Удосконалення адміністративно-правового забезпечення кібербезпеки в Україні: досвід європейських країн. *Наукові записки*. Серія: Право. 2023. № 14. С. 143-147.
24. Комих Н. Г. Актуальні аспекти кібербезпеки в Україні під час війни. Міжнародна та національна безпека: теоретичні і прикладні аспекти: матеріали VII Міжнар. наук.-практ. конф. (м. Дніпро, 17 бер. 2023 р.). Дніпро: ДДУВС, 2023. С. 530-532
25. Лесько, Н. В. Кібербезпека як частина національної безпеки України в умовах війни. *Юридичний науковий електронний журнал*. 2023. № 5. С. 224-226.
26. Мордань, Є. Ю. Удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству на основі впровадження міжнародного досвіду. *Ефективна економіка*. 2023. № 10. Електронний ресурс. URL: https://www.nayka.com.ua/index.php/ee/article/view/2329/2361
27. Лугіна Н.А., Бойко В.В. Європейський досвід подолання кіберзлочинності в Україні в умовах сьогодення. *Нове українське право*. 2022. Випуск 6, Том 2. С. 42-46;
28. Сємко М.О. Нормотворча діяльність ООН щодо забезпечення інформаційної безпеки у воєнній сфері. *Юридичний науковий електронний журнал*. 2022. № 8. С. 580–583.

29. Гавловська А.О. Стратонов В.М., Проценко М.В.Апаратні та програмні засоби для дослідження мобільних телефонів, sim-карт як елемент техніко-криміналістичного забезпечення розслідування кримінальних правопорушень. Proceedings of the 6th International scientific and practical conference. Bo Science Publisher. Chicago, USA. 2021. Pp. 1123–1131. URL: https://sci-conf.com.ua/vi-mezhdunarodnaya-nauchno-prakticheskaya-konferentsiyamodern-directions-of-scientific-research-development-24-26-noyabrya-2021-godachikago-ssha-arhiv/ ISBN 978-1-73981-126-6
30. Гавловська А.О., Проценко М.В.Застосування криміналістичної техніки під час досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Запорізького національного університету. Юридичні науки.* № 1, 2021. С. 87–93. DOI https://doi.org/10.26661/2616-9444-2021-1-014 ISSN 2616-9444 (Print) ISSN 2616-9452 (Online) (фахове видання) http://law.journalsofznu.zp.ua/visnik-1-2021 Журнал індексується в базі IIJIF