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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ Роман МАКСИМОВИЧ
«____»_____2022 р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»
спеціальності 293 «Міжнародне право»

Тема: **МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ СПІВРОБІТНИЦТВА ДЕРЖАВ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

Виконавець: ШУЛІЧЕНКО Максим Вікторович
Науковий керівник: к.ю.н., доцент ЛЕСЬ Ірина Олександрівна
Нормоконтролер: викладач ГОЛОВАТЕНКО Марина Юріївна

Київ, 2022

ЗМІСТ

ВСТУП

Актуальність обраної теми дослідження. Активне впровадження сучасних цифрових технологій в економічну, соціальну сфери, управління, кредитно-банківську діяльність, безпеку та оборону країни, стрімкий розвиток інформаційно-телекомунікаційних технологій (далі – ІКТ) на основі глобальної інформаційної мережі Інтернет надає доступ до неї широкому колу користувачів, що призводить до збільшення кількості ризиків і загроз, характерних для кібербезпеки та її складових.

Тим не менш, ІКТ є невід'ємною частиною майже будь-якої сфери існування окремих осіб і громадян, і їх захист потребує комплексного міждисциплінарного регулювання. В умовах всеосяжної глобалізації та стрімкого розвитку інформаційно-комунікаційних технологій жодна країна світу не може самостійно забезпечити надійну гарантію свого цифрового простору та забезпечити безпеку мережі. Однак повільний і непередбачуваний розвиток моделі міжнародної системи забезпечення безпеки у сфері інформаційних технологій значно підвищив важливість розвитку двосторонньої та багатосторонньої співпраці у формуванні єдиного стратегічного підходу. З огляду на це, усе більш актуальним стає питання формування єдиного правового простору для співробітництва держав щодо протидії злочинам у сфері інформаційних технологій.

Аналіз останніх досліджень та публікацій. Проблема розробки ефективного міжнародно-правового механізму протидії злочинам у сфері інформаційних технологій знайшла своє відображення в роботах багатьох вітчизняних та зарубіжних учених, серед них зокрема С. Гудман, Ф. Вільямс,

Д. Деннінг [1], Б. Колін [2], Л. Шеллі [3] та Д. Шиндер [4]. У вітчизняній доктрині питання кіберзлочинності досліджували: О. Бойченко [5], В. Брижко [6], В. Бутузов [7], А. Войціховський [8], В. Марков [9], М. Палієнко [10], Т. Сироїд [11], В. Сідак [12], М. Швець [13] та інші. Аналіз окремих складів злочинів, пов’язаних з використанням комп’ютерної техніки розглядалися у працях А. Васильєва [14], В. Голубєва [15], Ю. Максименко [16], В. Мещерякова [17], та інших науковців. Незважаючи на значний інтерес серед науковців до питань, пов’язаних із протидією злочинам у сфері інформаційних технологій, аналізу міжнародно-правового співробітництва країн у зазначеному напрямку приділяється менше уваги, незважаючи на його зростаючу актуальність.

Метою даної роботи є аналіз міжнародно-правового регулювання співробітництва держав щодо протидії злочинам у сфері інформаційних технологій.

Вказана мета обумовлює наступні **завдання**:

- розглянути теоретико-правові аспекти та міжнародно-правові засади міжнародного співробітництва щодо протидії злочинам у сфері інформаційних технологій;
- дослідити інституційні механізми співробітництва держав щодо протидії злочинам у сфері інформаційних технологій, сформовані Організацією Об'єднаних Націй, Європейським Союзом та Інтерполом;
- визначити перспективи вдосконалення механізмів міжнародно-правового співробітництва держав щодо протидії злочинам у сфері інформаційних технологій;
- окреслити пріоритетні напрями міжнародного співробітництва України у сфері забезпечення безпеки інформаційного простору.

Об’єктом дослідження є суспільні відносини у сфері міжнародно-правового регулювання співробітництва держав щодо протидії злочинам у сфері інформаційних технологій.

Предметом дослідження є комплекс теоретико-правових уявлень щодо міжнародно-правового регулювання співробітництва держав щодо протидії злочинам у сфері інформаційних технологій.

Методологічна основа роботи. Для досягнення наукових результатів використовуються в поєднанні загальнонаукові, конкретно-наукові та конкретно-наукові методи. Крім того, у процесі дослідження також застосовуються такі методи, як метод аналізу, метод узагальнення, метод дедукції, метод індукції, метод порівняння та метод структури системи.

Відповідно до загальнонаукового методу теоретичного дослідження, методологічною основою роботи є основні положення діалектичного методу пізнання, які можуть відображати співвідношення теорії і практики, форму і зміст навчальної дисципліни. Вивчати, аналізувати процес розвитку та якісну зміну соціально-правових явищ, форми і закону – за його допомогою визначати точні концептуальні формулювання.

У ході дослідження проаналізовано та узагальнено філософські, теоретико-правові та історичні, соціологічні дослідження, що відображають розвиток міжнародної правової системи.

Використовувати індуктивну та експертну оцінку для проведення дослідницької правової оцінки існуючої бази боротьби зі злочинністю у сфері інформаційних технологій.

Апробація результатів дослідження. Окремі наукові результати дослідження були апробовані та опубліковані у межах наступних науково-практичних конференціях:

- «Пріоритетні напрями міжнародного співробітництва України у сфері забезпечення безпеки інформаційного простору» (CXI Міжнародна інтернет-конференція «Жовтневі наукові читання», м. Івано-Франківськ);
- «Міжнародно-правові засади співробітництва держав щодо протидії злочинам у сфері інформаційних технологій» (Круглий стіл «Європейські стандарти освітніх програм: молодь і наука», м. Київ).

Структура роботи обумовлена її метою, завданнями та предметом дослідження. Дипломна робота складається зі вступу, трьох розділів, якими охоплюються сім підрозділів, висновків та списку використаних джерел (101 найменування). Загальний обсяг дипломної роботи –74 сторінки, у тому числі список використаних джерел – 12 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ФОРМУВАННЯ ЮРИДИЧНИХ ЗАСАД СПІВРОБІТНИЦТВА ДЕРЖАВ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1. Теоретико-правові аспекти міжнародного співробітництва щодо протидії злочинам у сфері інформаційних технологій

З виникненням нових інформаційних технологій та процесів з'явилася нагальна потреба у їх правовому регулюванні. І хоча право є універсальним регулятором суспільних відносин, саме у сфері комп'ютерної інформації воно виявилося не цілком готовим до нових викликів.

З 80-х років. XX ст. у багатьох країнах дійшли висновку, що правовий захист комп'ютерної інформації за допомогою загальних положень національного кримінального законодавства є недостатнім. Багато держав усвідомили, що ефективне вирішення проблеми комп'ютерної злочинності потребує узгоджених міжнародних дій та співробітництва. Так, на Генеральній Асамблеї ООН у вересні 1991 р. зазначалося, що «зростання злочинності у поєднанні з процесом набуття нею транснаціонального характеру ставить під загрозу внутрішню безпеку держав, зазіхає на свободу людини жити без страху, а також може підірвати міжнародні відносини. Все це потребує ефективних міжнародних механізмів та більш тісної співпраці між державами» [18].

Однак для того, щоб розробляти спільні міжнародні норми та нові механізми, необхідний уніфікований підхід до розуміння проблеми,

формування єдиної мети та універсальних принципів. На даний момент аналіз закордонного кримінального законодавства показує, що відсутнє однакове розуміння того, які дії вважати комп'ютерними злочинами і яке має бути юридичне визначення кожного з них. Від різних підходів до поняття та складів комп'ютерних злочинів виникають складнощі у виявленні та покаранні злочинців, коли саме діяння має місце в одній країні, а його наслідок настає в іншій, де таке діяння може бути кримінально-карним [19].

Неузгоджений підхід не сприяє ефективній протидії комп'ютерним злочинам. Через це міжнародно-правові механізми мають відігравати головну роль у процесі уніфікації національного кримінального законодавства різних країн у цій сфері, у тому числі і у прийнятті спільних понять.

У 1983-1985 р.р. в Організації економічного співробітництва та розвитку (далі - ОЕСР) було створено спеціальний комітет для обговорення можливості узгодження кримінального законодавства різних країн щодо відповідальності за комп'ютерні злочини. ОЕСР за результатами роботи рекомендувала віднести до кримінально-карних діянь такі дії [20]:

1) запровадження, зміна, стирання та/або пошкодження комп'ютерних даних та/або комп'ютерних програм, що здійснюється навмисне з наміром здійснити незаконне переведення фінансових коштів або інших цінностей;

2) введення, зміна, стирання та/або пошкодження комп'ютерних даних та/або комп'ютерних програм, що здійснюється навмисне з наміром вчинити підробку;

3) введення, зміна, стирання та/або пошкодження комп'ютерних даних та/або комп'ютерних програм, або інші маніпуляції з комп'ютерними системами, що здійснюється навмисно з наміром перешкодити функціонуванню комп'ютера та/або телекомунікаційної системи;

4) порушення виключного права власника комп'ютерної програми, що охороняється авторським правом, з наміром скористатися програмою в комерційних цілях і реалізувати її на ринку;

5) доступ до комп'ютера та/або до телекомунікаційної системи та перехоплення інформації, що видається комп'ютером та/або телекомунікаційною системою, який був отриманий як наслідок усвідомленої дії без дозволу особи, відповідальної за функціонування системи, шляхом порушення охоронних заходів або інших нечесних чи зловмисних дій.

Першим документом Ради Європи, присвяченим комп'ютерній злочинності, стала Рекомендація № R 89(9) Комітету Міністрів країн - членів Ради Європи про злочини, пов'язані з комп'ютером, прийнята 13.09.1989 року, в якій було використано такий термін, як «злочин, пов'язаний з використанням комп'ютерних технологій» [21]. Цей документ містив перелік рекомендованих до обов'язкового включення до національного кримінального законодавства діянь. Крім того, наводився перелік тих діянь, за якими не було досягнуто згоди у визнанні необхідності їхньої криміналізації у законодавстві всіх країн.

До переліку правопорушень, рекомендованих до обов'язкового включення до внутрішньодержавного кримінального законодавства відповідно до зазначеної Рекомендації, віднесено:

а) Комп'ютерне шахрайство. Введення, зміна, стирання або пошкодження комп'ютерних даних або комп'ютерних програм або інше втручання в процес обробки даних, що впливає на результат обробки даних та завдає економічної шкоди або призводить до втрати власності іншої особи, з наміром отримати незаконним шляхом економічну вигоду для себе або іншої особи.

б) Комп'ютерне підроблення. Введення, зміна, стирання або пошкодження комп'ютерних даних або комп'ютерних програм або інше втручання в процес обробки даних, що здійснюється таким способом або за таких умов, як це встановлюється національним законодавством, за яких ці діяння кваліфікувалися б як фальсифікація, вчинена щодо традиційного об'єкта такого правопорушення.

в) Заподіяння шкоди комп'ютерним даним або комп'ютерним програмам. Протиправне стирання, заподіяння шкоди, погіршення якості або пошкодження комп'ютерних даних або програм.

г) Комп'ютерний саботаж. Введення, зміна, стирання або пошкодження комп'ютерних даних або комп'ютерних програм, створення перешкод комп'ютерним системам з наміром перешкодити роботі комп'ютера або телекомунікаційної системи.

д) Несанкціонований доступ. Неправомірний доступ до комп'ютерної системи або мережі через порушення охоронних заходів.

є) Несанкціоноване перехоплення. Неправомірне та здійснене за допомогою технічних засобів перехоплення повідомлень, що надходять у комп'ютерну систему або мережу, що виходять із комп'ютерної системи чи мережі та передаються в рамках комп'ютерної системи чи мережі.

ж) Несанкціоноване відтворення комп'ютерної програми, що охороняється авторським правом. Неправомірне відтворення, розповсюдження або передача у громадське користування комп'ютерної програми, що охороняється законом.

з) Несанкціоноване відтворення мікросхеми. Неправомірне відтворення мікросхеми виробу, що охороняється законом, на напівпровідниках або неправомірне комерційне використання або імпорт з цією метою мікросхеми або виробу на напівпровідниках, виготовленого з використанням цієї мікросхеми.

Серед спірних складів злочинів названо:

а) Зміна комп'ютерних даних чи комп'ютерних програм. Неправомірна зміна комп'ютерних даних або програм.

б) Комп'ютерне шпигунство. Придбання недозволеними методами або розкриття, передача або використання торгової або комерційної таємниці, не маючи на це права або будь-якого іншого правового обґрунтування, з метою заподіяти економічні збитки особі, яка має доступ до цієї таємниці, або отримати незаконну економічну вигоду для себе або третьої особи.

в) Несанкціоноване використання комп'ютера. Неправомірне використання комп'ютерної системи або мережі, що відбувається: або 1) з розумінням того, що особа, яка має право на використання системи, зазнає значного ризику шкоди або системі або її функціонуванню, або 2) з наміром заподіяти шкоду особі, яка має право на використання системи, або системі чи її функціонуванню, або 3) завдає шкоди особі, яка має право на використання системи, або системі чи її функціонуванню.

г) Несанкціоноване використання комп'ютерної програми, що охороняється законом. Неправомірне використання комп'ютерної програми, що охороняється законом і яка відтворюється без права на відтворення, з наміром забезпечити незаконний економічний прибуток для себе або іншої особи або завдати шкоди власнику відповідного права [22].

Рекомендація № R 89(9) передбачила, що у положеннях кримінального закону повинні міститися якомога точніші описи кримінально-караних діянь. Цей принцип ясності є надзвичайно важливим, але, на жаль, не всі держави його дотримуються (зокрема Росія його не визнала) [23].

У той же час, вищезгадана Рекомендація сама не містила чіткого формулювання поняття «злочин, пов'язаний з використанням комп'ютерних технологій». Воно виводилося з переліку діянь, зазначених у Рекомендації та дає уявлення про вище перелічені злочини.

Цей документ став орієнтиром для багатьох європейських країн у вдосконаленні кримінального законодавства, і водночас сприяв зближенню національного кримінального законодавства різних країн.

Але необхідно враховувати, що цей документ має лише рекомендаційний характер. І не зважаючи на позитивний вплив, не з усіх принципових питань європейські держави досягли достатнього зближення. На практиці це призвело до проблем узгодженої боротьби зі злочинами у сфері комп'ютерних технологій. Крім цього, недоліком Рекомендації було і те, що в ній не було кримінально-процесуальних норм [24].

Наступним кроком у розвитку міжнародного співробітництва у боротьбі з комп'ютерними злочинами стала розробка на початку 90-х років робочою групою Міжнародної організації кримінальної поліції Інтерпол (далі - Інтерпол) кодифікатора комп'ютерних злочинів, у подальшому кодифікатор був покладений в основу автоматизованої інформаційно-пошукової системи. Цей кодифікатор застосовується при надсиланні запитів та повідомлень про злочини у сфері комп’ютерних технологій через мережу Міжнародної організації кримінальної поліції Інтерпол.

Відповідно до названого кодифікатора всі комп'ютерні злочини класифіковані таким чином [25]:

1.QA - Несанкціонований доступ та перехоплення: комп'ютерний абордаж (хакінг), несанкціонований доступ до комп'ютерної інформації або мережі, перехоплення інформації та ін.

2.QD - Зміна комп'ютерних даних: логічна бомба, троянський кінь, «хробак», комп'ютерний вірус та ін.

3.QF - Комп'ютерне шахрайство: шахрайство з банкоматами, з ігровими автоматами, з платіжними засобами, телефонне шахрайство та ін.

4.QR - Незаконне копіювання: копіювання комп'ютерних ігор, програмного забезпечення, топології напівпровідникових пристроїв та ін.

5.QS - Комп'ютерний саботаж: порушення роботи електронної обчислювальної машини, знищення, блокування інформації та ін.

6.QZ - Інші комп'ютерні злочини: розкрадання інформації, що становить комерційну таємницю (комп'ютерне шпигунство), використання комп'ютерних дощок оголошень для злочинної діяльності та ін.

За цим переліком можна будувати висновки про те, що до злочинів у сфері комп'ютерної інформації належить дуже широкий спектр діянь. Але, знову ж таки, не всі ці дії сприйняті в національних законодавствах, як злочинні діяння.

У рамках Групи Восьми (G-8) [26] протягом 90-х років проводилося безліч нарад щодо проблеми комп'ютерної злочинності. Зокрема, у липні

2000 р. на Окінаві (Японія) відбулася чергова нарада керівників глав держав та урядів Групи Восьми. Було визнано необхідним «прийняти спільний підхід у сфері боротьби зі злочинами в галузі високих технологій, такими як кіберзлочини, які можуть серйозно загрожувати безпеці та довірі у глобальному інформаційному просторі» [27]. І такий загальний підхід отримав відображення у прийнятій на цій нараді «Окінавській Хартії про глобальне інформаційне суспільство», в якій зазначено: «Зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, повинні супроводжуватися узгодженими діями щодо створення безпечного та вільного від злочинності кіберпростору…» [28].

Додатковий протокол II до Конвенції про кіберзлочинність (Будапештська конвенція), спрямований на посилення співпраці та розкриття електронних доказів, був відкритий для підписання на зустрічі, організованій Італією під час її головування в Комітеті міністрів Ради Європи.

Протокол був підписаний такими державами-членами Європейської Комісії в присутності кількох міністрів: Австрія, Бельгія, Болгарія, Естонія, Фінляндія, Ісландія, Італія, Литва, Люксембург, Чорногорія, Нідерланди, Північна Македонія, Португалія, Румунія, Сербія, Іспанія і Швеція, а також країнами, що не є членами: Чилі, Колумбія, Японія, Марокко та Сполучені Штати [29].

Угода передбачає інструменти для посилення співпраці та розкриття електронних доказів, такі як пряма співпраця з постачальниками послуг і реєстраторами, ефективні засоби отримання інформації про користувачів і трафіки, негайна співпраця у надзвичайних ситуаціях або спільне розслідування з урахуванням прав людини та верховенства права, включаючи гарантії захисту даних.

Отже, сучасні можливості та ускладнення соціальних відносин, активізація транскордонної злочинності та розвиток технологій призвели до появи такого явища, як злочини у сфері інформаційних технологій. Довгий

час сфера була практично вільною від міжнародного права, але на сьогоднішній день розроблено чимало норм, спрямованих на боротьбу зі злочинністю у сфері високих технологій. Проте існуюча галузь міжнародного права є недостатньо ефективною та не має одноманітності та одностайності правового регулювання в конкретній галузі. Це в першу чергу проявляється у використанні різної термінології та концептуальних засобів таксономії. Тому розробка загального та уніфікованого визначення поняття «кіберзлочинність» є першим кроком до кримінально-правової боротьби зі злочинами у сфері інформаційних технологій.

1.2. Міжнародно-правові засади співробітництва держав щодо протидії злочинам у сфері інформаційних технологій

Незважаючи на те, що злочини у сфері інформаційних технологій з'явилися відносно нещодавно, вони перетворилися з незаконного діяння в одну з найбільших загроз сучасної цивілізації. З кожним роком явище кіберзлочинності набирає обертів і стає все більш поширеним видом злочинності, що потребує розробки відповідної правової теорії та методологічного інструментарію, насамперед науки кримінального права.

Більшість злочинів у сфері інформаційних технологій, як нами зазначалося вище, здійснюються не лише на території чи віртуальному просторі окремої країни, вони також можуть мати більш глобальний, міждержавний чи навіть міжнародний характер. Власне, це породжує потребу в міжнародній співпраці, оскільки однією з головних проблем, з якою стикаються співробітники правоохоронних органів під час розслідування злочинів у сфері інформаційних технологій, є складність визначення особи злочинця, територіального розташування його країни та правил закону, згідно з яким порушник може бути притягнутий до кримінальної відповідальності[30].

Подальший розвиток міжнародного співробітництва у справі протидії злочинам у сфері інформаційних технологій спрямований на вирішення трьох завдань: персоналізація особи злочинця, визначення юрисдикції та головне – обрати для правопорушника найбільш прийнятні заходи юридичної відповідальності, щоб притягнути його до відповідальності за вчинення цього злочину.

Усі міжнародні організації вказують на необхідність скоординованої міждержавної співпраці у розслідуванні злочинів у сфері інформаційних технологій. Завдяки роботі Організації економічного співробітництва та розвитку (далі – ОЕСР), Інтерполу, «Великої вісімки» (далі – G8), Ради Європи, ООН та інших міжнародних організацій, розвивається міжнародне співробітництво країн у сфері боротьби з кіберзлочинністю, формується законодавство.

Однак для формулювання та реалізації міжнародно-правових норм необхідний єдиний підхід до розуміння питань, визначення спільних завдань і формулювання загальних принципів. Кримінальне законодавство різних країн має непослідовні методи формулювання конкретних злочинів, що не сприяє застосуванню ефективних заходів протидії комп'ютерним злочинам у глобальному масштабі. У зв'язку з цим важливу роль у координації національного кримінального законодавства з міжнародно-правовими актами, сформульованими та прийнятими відповідними організаціями, мають відігравати міжнародні закони та нормативні акти [31].

Розглядаючи зародження міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю в останні роки, зазначимо, що ще у квітні 1995 року відбулася перша Міжнародна конференція INTERPOL з комп'ютерних злочинів [32].

У 1996 році «Велика вісімка» вирішила створити групу, яка займатиметься боротьбою з міжнародними злочинами у сфері інформаційних технологій – «Ліонська група». Тим часом глави держав затвердили план боротьби з кіберзлочинністю. Серед найважливіших пунктів документу варто

відзначити: створення в кожній країні цілодобового контакт-центру для взаємодії у боротьбі зі злочинами у сфері інформаційних технологій, надання допомоги іншим країнам кваліфікованими правоохоронцями, розвиток спільного Стандарту щодо отримання та перевірки автентичності електронних даних і ознайомлення із законодавчим підходом до боротьби з комп'ютерними злочинами в країнах-учасницях [33].

У 2000 році на Десятому Конгресі з попередження злочинності та поводження з правопорушниками, що проходив в рамках ООН, було підкреслено, що постійне зростання глобальної кіберзлочинності, поява нових видів злочинів у сфері інформаційних технологій, а також нездатність країн і організацій співпрацювати в рамках національного та міжнародного права породжує дедалі більше проблем у правовій площині.

У березні 2001 року Комісія ООН із запобігання злочинності та кримінального правосуддя представила спеціальну доповідь, у якій вперше була запропонована класифікація злочинів у сфері інформаційних технологій [34].

Не менш важливим документом в рамках ООН є Резолюція 2001 року «Про боротьбу з незаконним використанням інформаційних технологій» [35]. У ній наголошується на необхідності співпраці між державою та приватним сектором у боротьбі з незаконним використанням інформаційних технологій, що має досягатися шляхом: включення відповідальності за інформаційні злочини до законодавства; транснаціональної співпраці між правоохоронними органами; міжнародного обміну інформацією з використання інформаційних технологій для боротьби зі злочинністю; підготовка працівників правоохоронних органів в умовах інформаційного суспільства; захист комп’ютерних систем від несанкціонованого втручання тощо.

Крім того, слід звернути увагу на пункт 1 Резолюції, в якому йдеться про те, що розвиток інформаційних технологій має сприяти запобіганню та виявленню випадків злочинного використання, відстеженню злочинців та

збору доказів. Теоретично проект дає правоохоронним органам іншої країни можливість виявляти їх і Організація вживає заходів для затримання злочинців на короткі терміни, що дозволить досягати високих результатів. Однак злочинці можуть отримати незаконний доступ до вищезгаданих технологій і використовувати приховані можливості системи для вчинення злочинів у сфері інформаційних технологій, таких як викрадення персональних даних.

Сьогодні Основним документом, що регулює міжнародне співробітництво у сфері запобігання та боротьби з кіберзлочинністю, є Конвенція про кіберзлочинність (далі – Конвенція), підписана в Будапешті 23 листопада 2001 року. Конвенція встановлює найзагальніші положення, а також визначає принципи щодо заходів боротьби з кіберзлочинністю на національному та міжнародному рівнях.

Відповідно до ст. 23 Конвенції сторони максимально можливо співпрацюють одна з одною у розслідуванні або судовому переслідуванні кримінальних правопорушень, пов’язаних зі злочинністю, шляхом застосування міжнародних документів про співпрацю в міжнародних кримінальних справах, угодах, укладених на основі єдиного або спільного внутрішнього законодавства з використанням комп’ютерних систем та даних для збору доказів в електронній формі у зв’язку з кримінальними злочинами [36].

Конвенція розрізняє чотири категорії злочинів проти конфіденційності, цілісності та доступності комп’ютерних даних і систем:

1. Злочини у сфері незаконного доступу до інформації: незаконне перехоплення (ст. 3), втручання в дані (ст. 4), втручання в роботу систем (ст. 5), неправомірне використання обладнання (ст. 6);
2. Злочини, пов'язані з незаконним використанням комп'ютерів: комп'ютерне підроблення (ст. 7), комп'ютерне шахрайство (ст. 8);
3. Злочини, пов’язані з контентом, у тому числі виготовлення, розповсюдження та зберігання дитячої порнографії (стаття 9);

4. Правопорушення, пов’язані з порушенням авторського права і суміжних прав (ст. 10) [35].

У цьому випадку виникає одна з перших проблем міжнародного співробітництва, оскільки правовий вплив, проголошений у Конвенції, не відповідає реальним сучасним умовам розвитку кіберзлочинності: вперше виникає не лише кіберзлочинність, а й її крайній прояв – доктрина кібертероризму. У відповідь на це вчені розробили класифікацію джерел кіберзлочинності, щоб якнайшвидше виявляти загрози та вживати необхідних заходів для їх усунення. Враховуючи це, експерти поділяють осіб та організації, які здійснюють атаки, на категорії, з яких формується сама кіберзлочинність [37]:

- Хакер – це людина, яка має високий рівень знань у галузі комп’ютерних технологій і проводить багато часу за комп’ютерами, шукаючи слабкі місця в комп’ютерних системах (вчинення злочинних дій, таких як DoS-атаки, дефейс, розповсюдження шкідливих програм тощо);
- Хактивісти, чия діяльність є поєднанням соціальної активності, спрямованої проти чогось, і хакерство (використання інтернет-технологій для завдання шкоди комп’ютерним мережам та їх користувачам). Характеризується такими злочинами, як розповсюдження шкідливих програм (вірусів), особисті образи та наклеп; фактично є кіберзлочинцями, діяльність яких спрямована на отримання неправомірної вигоди (їм притаманні такі злочини, як крадіжка карток, фішинг, інтернет-шахрайство тощо);
- Професіонали, які займаються промисловим шпигунством;
- Кібертерористи, діяльність яких пов'язана з різними проявами екстремізму в мережі. Сьогодні терористи досягли такого рівня, коли вони можуть використовувати Інтернет (самостійно чи в поєднанні з фізичними атаками) як інструмент для завдання реальної шкоди.

Важливим аспектом, на якому слід зосередитися при дослідженні Конвенції, є те, що вона приділяє особливу увагу співучасті в кіберзлочинах, наголошуючи на відповідальності за замах і пособництво (ст. 11) та спільну відповідальность за співучасть (ст. 12).

Що стосується санкцій за вчинення цих злочинів, то в статті 13 Конвенції зазначено, що кожна держава, яка ратифікувала Конвенцію, вживає необхідних законодавчих та інших заходів для забезпечення того, щоб кримінальні правопорушення, визначені статтями 2-11 Конвенції, підлягали ефективним, пропорційним і переконливим санкціям, включаючи позбавлення волі. Також зазначено, що відповідальність юридичних осіб необхідно забезпечувати на основі ефективних, пропорційних і переконливих кримінальних або некримінальних санкцій або заходів, у тому числі грошових санкцій.

Відповідно до ст. 15 Конвенції кожна держава, яка ратифікує Конвенцію, забезпечує встановлення, реалізацію та застосування повноважень і процедур, викладених у Конвенції, відповідно до умов і гарантій, встановлених національним законодавством для забезпечення повного захисту прав і свобод людини. Конвенція передбачає такі види превентивних заходів [35]:

- загальні заходи, включаючи термінове збереження комп'ютерних даних (ст. 16), а також екстрене збереження та часткове розкриття даних про рух інформації (ст. 17);

- заходи доручення (ст. 18), які встановлюють процедури та обмеження для видачі 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 збір даних про рух інформації в реальному часі (ст. 20) та перехоплення даних інформаційного змісту (ст. 21).

Що стосується процесу міжнародного співробітництва у сфері безпосередньої боротьби з кіберзлочинцями (оперативна діяльність правоохоронних органів), то Конвенція передбачає, зокрема, такі заходи [35]:

- екстрадиція (ст. 24);

- взаємна допомога (ст. 25), коли обидві сторони надають взаємну допомогу в максимально можливому обсязі для розслідування або судового переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, або з метою збору доказів в електронній формі про злочинців;

- добровільна допомога (ст. 26), коли сторона може в рамках свого законодавства та без попереднього запиту надіслати іншій стороні інформацію, отриману в ході власного розслідування, якщо вона вважає, що розкриття такої інформації може допомогти стороні в отриманні інформації в контексті виявлення або проведення розслідування чи судового переслідування, пов'язаного з кіберзлочинністю;

- взаємна допомога щодо тимчасових заходів, включаючи термінове збереження збережених комп'ютерних даних (ст. 29) та термінове розкриття збережених даних, пов'язаних з переміщенням інформації (ст. 30);

- взаємна допомога щодо слідчих повноважень, а саме: взаємна допомога в доступі до збережених комп'ютерних даних (ст. 31); транскордонний доступ до відкритих або загальнодоступних комп'ютерних даних (ст. 32);

- взаємна допомога в зборі даних потоку інформації в режимі реального часу (ст. 33);

- взаємодопомога у перехопленні інформаційний даних (ст. 34);

- цілодобова мережа, тобто створення та підтримка мережі, в якій здійснюється обмін різноманітною інформацією щодо запобігання кіберзлочинам (ст. 35).

Беручи до уваги питання боротьби з кіберзлочинністю, крізь призму Конвенції можна зробити висновки щодо питання загальних позицій щодо

того, яку поведінку, пов’язану з використанням комп’ютерних систем, слід криміналізувати.

По-перше, такі дії вважаються кримінальними діями, що дозволяє застосовувати силу, необхідну для ефективної боротьби з ними, а також заходи, необхідні для виявлення, розслідування та судового переслідування таких злочинів як усередині країни, так і на міжнародному рівні.

По-друге, наявність у Конвенції положення про «обшук і конфіскацію збережених комп’ютерних даних» дозволяє одній стороні забезпечити збереження важливої інформації, необхідної для розслідування злочину, яка знаходиться в межах юрисдикції іншої сторони. Зрозуміло, що інтернет-провайдери часто мають дані про минулі обміни інформацією, які можна отримати за допомогою обладнання, яке записує конкретні аспекти обміну інформацією, включаючи час, тривалість і дату будь-яких повідомлень. Зазвичай такі дані зберігаються протягом обмеженого періоду часу, залежно від комерційних потреб оператора чи постачальника послуг, а також вимог законодавства щодо нерозголошення приватної інформації.

Національне законодавство багатьох країн дозволяє правоохоронним або судовим органам видавати накази щодо збору, даних обміну інформацією. Важливим положенням Конвенції є те, що вона може вживати законодавчих та інших заходів для надання повноважень компетентним органам конфіскувати або подібним чином захищати дані від знищення, які необхідні для володіння постачальника та дослідження [38].

Безсумнівно, з юридичної точки зору загальні принципи міжнародного співробітництва, визначені в Конвенції, є дуже важливими. Йдеться про екстрадицію злочинців у сфері інформаційних технологій, при цьому країни надають широку взаємну допомогу одна одній у розслідуванні кримінальних справ, пов’язаних із комп’ютерними системами та даними, а також у зборі електронних доказів.

Враховуючи специфіку соціального явища кіберзлочинності, масштаби інформатизації та розвиток глобальної мережі Інтернет, стає все менш

вірогідним, що такі злочини обмежуються територією однієї країни. Під час проведення розслідувань правоохоронні органи в різних країнах повинні співпрацювати один з одним, формально використовуючи рамки та структури, такі як Інтерпол, або неофіційно, безпосередньо надаючи національним правоохоронним органам потенційно корисну інформацію.

Інші додаткові питання неминуче виникають, коли мова йде про правову допомогу під час розслідування злочинів у сфері інформаційних технологій. Якщо внутрішнє законодавство країни не передбачає конкретних повноважень для отримання доказів в інформаційних мережах, такі сторони не зможуть адекватно реагувати на прохання іншої сторони про допомогу. У зв'язку з цим важливою умовою міжнародного співробітництва є координація всіх сторін щодо вжиття необхідних заходів для розслідування злочинів у сфері інформаційних технологій [39].

Слід зазначити, що в деяких країнах Західної Європи існує правовий принцип, згідно з яким країна може здійснювати юрисдикцію над територією іншої країни, якщо вона незаконно порушує інтереси іншої країни. Однак в ЄС звертають увагу на те, що це положення потребує міжнародного регулювання, оскільки країни часом надто широко трактують норми цієї доктрини. Сьогодні першочерговим завданням міжнародного співробітництва є уніфікація національного кримінального законодавства країн, які беруть участь у процесі міжнародного співробітництва у сфері протидії кіберзлочинності, навіть за наявності конвенцій.

Тенденція до зростання кіберзлочинності та «відстала» тенденція соціально-правового контролю сформували велику загрозу цивілізації, подолати яку можна лише шляхом боротьби з цим видом кіберзлочинності шляхом органічного поєднання кримінально-правових та судових стратегій. Крім того, важливою частиною цієї стратегії має бути більш прозора та ефективна міжнародна співпраця у цій сфері, оскільки неможливо контролювати транснаціональні складові кіберзлочинності та кібертероризму

на рівні окремих країн. Дійсно, у XXI столітті міжнародне співтовариство має терміново вирішити цю складну проблему.

Враховуючи вище викладене, можна підсумувати, що виникнення та подальший розвиток міжнародного співробітництва у сфері протидії кіберзлочинності спрямоване на вирішення трьох завдань: персоналізація особи правопорушника, встановлення юрисдикції та, головне, вибір правового впливу на правопорушника, який є найбільш адекватним для того, щоб викликати у нього відчуття провини за вчинення цього злочину та подібних злочинів.

РОЗДІЛ 2. СИСТЕМА ІНСТИТУЦІЙНИХ МЕХАНІЗМІВ СПІВРОБІТНИЦТВА ДЕРЖАВ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1. Інституційний механізм співробітництва держав щодо протидії злочинам у сфері інформаційних технологій, сформований Організацією Об'єднаних Націй

Епоха інформаційних технологій разом із досягненнями, пов’язаними з використанням її плодів, породила нову форму злочинності – кіберзлочинність, реалізація якої зачіпає інтереси окремих осіб, націй і міжнародного співтовариства в цілому, а також оскільки інформаційні технології використовуються для злочинів, їх наслідки далеко за межами країни становлять загрозу економічному розвитку, політичної стабільності та створюють умови для соціальної напруги.

Питання боротьби з незаконним використанням інформаційних технологій виходить за рамки національного регулювання і обговорюється на міжнародному рівні. Основні установи ООН зробили значний внесок у

регулювання інформаційно-комунікаційних технологій та забезпечення безпеки їх учасників.

Перш за все, необхідно зосередитися на діяльності Генеральної Асамблеї, яка розглядає широке коло питань, зокрема: створення правової бази для боротьби з нелегальним використанням ІКТ, становлення глобальної культури кібербезпеки, досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки, ІКТ для розвитку тощо (рез.: 53/70, 54/49, 55/28, 55/63, 56/19, 56/121 57/53, 57/173, 57/239, 58/136, 59/ 6160/45, 61/54, 62/17, 63/37, 64/25, 65/41, 66/24, 67/27, 68/243, 69/28, 69/204, 70/237).

У 2000 році Генеральна Асамблея прийняла резолюцію A/RES/55/63 про боротьбу з незаконним використанням інформаційних технологій, яка містила кілька рекомендацій, зокрема: створення умов на національному рівні, які б не дозволяли особам зловживати інформаційними технологіями для приховування; співробітництво правоохоронних органів у справах про злочини, пов’язані з інформаційними технологіями; обмін інформацією між країнами щодо проблем, з якими стикаються країни у боротьбі з цими злочинами; відповідна професійна підготовка співробітників правоохоронних органів для боротьби зі злочинністю; зловживання інформаційними технологіями; правові системи для забезпечення безпеки даних комп’ютерних систем; здатність захистити конфіденційність, цілісність і доступність від несанкціонованого втручання, встановити в національному законодавстві покарання за жорстоке поводження у злочинних цілях тощо [40].

Резолюція A/RES/56/121 від 2002 року про боротьбу з незаконним використанням інформаційних технологій обговорювала існуючі міжнародно-правові підходи до боротьби з кіберзлочинністю та висвітлювала різні рішення. Підкреслює важливість міжнародних та регіональних міжнародних організацій у боротьбі зі злочинністю у секторі високих технологій, зосереджуючи увагу на діяльності Ради Європи; вказує на

необхідність національного законодавства, політики та практики для боротьби з незаконним використанням інформаційних технологій, враховувати міжнародний досвід у цій сфері [41].

2002 рік також ознаменувався прийняттям Генеральною Асамблеєю резолюції A/RES/57/239, яка підкреслила, що національні агентства, інші організації та окремі користувачі інформаційних систем і мереж, що розвиваються, дотримуються культури кібербезпеки, володіють і забезпечують доступ, управління, обслуговування та використання («учасники»). Призначені особи зобов'язані дотримуватися наступних додаткових вимог: а) учасники розуміють потребу в безпеці інформаційної системи, мережі та те, що вони можуть її покращити; б) брати відповідальність за безпеку інформаційних систем та мереж відповідно до своїх відповідних ролей . Їх політика, практика, заходи та процедури повинні бути доступні для періодичного перегляду та оцінки придатності для середовища їх застосування; в) вживати своєчасних і спільних заходів для запобігання інцидентам, виявлення інцидентів і реагування, якщо воні впливають на безпеку; г) враховувати законність інших інтересах, і розуміти, що їхні дії чи бездіяльність можуть завдати шкоди іншим учасникам; д) забезпечувати безпеку відповідно до прийнятих цінностей демократичного суспільства, включаючи свободу обміну ідеями та планами, вільний потік інформації, а також конфіденційність інформації та комунікацій, адекватний захист, відкритість і розкриття особистої інформації; е) учасники проводять регулярні оцінки ризиків, які: дозволяють ідентифікувати загрози та фактори вразливості; достатньо для охоплення ключових внутрішніх і зовнішніх факторів, таких як технічні, фізичні та людські фактори, що впливають на фактори безпеки, застосовані методи та сторонні послуги; може визначити прийнятний рівень ризику; допомогти вибрати відповідні інструменти контролю для контролю ризику потенційного пошкодження інформаційних систем і мереж, беручи до уваги характер і важливість інформації, яка має бути захищеною; є) розглядати безпеку як найважливіший фактор у

плануванні та проектуванні, експлуатації та використанні інформаційних систем і мереж; ж) приймати комплексний підхід до управління безпекою на основі динамічної оцінки ризику, що охоплює всі рівні та аспекти діяльності учасників; з) переглядати та перевіряти безпеку інформаційних систем і мереж, вносячи відповідні зміни в політику, практику та заходи безпеки, беручи до уваги нові загрози та ризики, що виникають [42].

Резолюція Генеральної Асамблеї A/RES/58/140 (с. 2)[43] приділила увагу питанню боротьби з незаконним використанням інформаційних технологій.

Резолюція Генеральної Асамблеї A/RES/58/199 підкреслила необхідність захисту інформаційної інфраструктури, запропонувавши кілька елементів для захисту найважливіших з них, зокрема: наявність мережі для негайного попередження про лазівки в кібернетиці, загрози та середовище інцидентів; підвищення обізнаності зацікавлених сторін для кращого розуміння природи та масштабів своєї критично важливої інформаційної інфраструктури та ролі, яку кожна з них повинна відігравати в забезпеченні безпеки цієї інфраструктури; забезпечення адекватними матеріалами та процедурами Закони та кваліфікований персонал, щоб держави могли розслідувати спроби порушення захисту найважливіших інформаційних структур і притягнення причетних до відповідальності; створення та забезпечення функціонування систем зв'язку та кризових ситуацій і перевірка їх функціонування для забезпечення їх використання в надзвичайних ситуаціях; забезпечення надійної та стабільної роботи в різних умовах; співпраця між країнами спрямована на відстеження спроб злому найважливіших інформаційних структур тощо [44].

У своїй резолюції A/RES/63/195 Генеральна Асамблея звернула увагу на злочини у сфері інформаційних технологій як на одне з нових політичних питань у сфері запобігання злочинності й кримінального правосуддя і налала рекомендації Управлінню ООН з наркотиків і злочинності (ЮНОДК) дослідити в рамках свого мандату шляхи і способи його вирішення [45].

На Всесвітньому саміті з питань інформаційного суспільства (Женева 2003 р. – Туніс 2005 р.) було порушено питання регулювання інформаційного простору та створення інформаційного суспільства для «побудови інформаційного суспільства, орієнтованого на інтереси людей», відкрите для всіх, спрямоване на розвиток суспільства, в якому кожен може створювати, отримувати доступ, використовувати та обмінюватися інформацією та знаннями, щоб окремі особи, громади та народи мали можливість повністю реалізувати свій потенціал для свого сталого розвитку та підвищення якості життя» [46].

За підсумками Женевської фази Всесвітнього саміту найвищого рівня, що відбулася 12 грудня 2003 р., була прийнята Декларація принципів «Розбудова інформаційного суспільства є глобальним завданням нового тисячоліття», яка стала для нового життя інформаційного суспільства [47]. У рамках цього ж етапу було прийнято План дій, який є розвиваючою основою для забезпечення прогресу до інформаційного суспільства на національному, регіональному та міжнародному рівнях, визначені за часом цілі сприятимуть реалізації концепції відкритого та справедливого інформаційного суспільства для всіх [48].

Туніський етап Всесвітнього саміту 2005 року ознаменувався прийняттям Туніського плану для інформаційного суспільства, який вказав на перехід від принципів до дії з урахуванням Женевського плану дій, зосередивши увагу на фінансових механізмах для подолання «цифрового розриву», щодо регулювання використання Інтернету та пов’язаних з цим питань, виконання рішень, прийнятих у Женеві та Тунісі [49].

Для координації виконання рішень Всесвітньої конференції на найвищому рівні Координаційний комітет глав систем ООН створив Групу інформаційного суспільства (2006) як міжвідомчий механізм. У своєму робочому плані на 2014-2015 роки він вирішив зосередити свою діяльність на координації сприяння ІКТ у порядку денному розвитку після 2015 року (пункт 42) [50].

У своїй резолюції A/RES/65/230 Генеральна Асамблея звернулася до Комісії з попередження злочинності та кримінального правосуддя з проханням створити міжурядову групу експертів відкритого складу відповідно до пункту 42 Сальвадорської декларації про комплексний підхід до глобальних загроз: системи запобігання злочинності та кримінального правосуддя та їх розвиток у мінливому світі, проведення всебічного дослідження кіберзлочинності та пов'язаних із ними дій держав-членів, міжнародної спільноти та приватного сектору, включаючи обмін інформацією про національне законодавство, найкращі практики, технічну допомогу міжнародне співробітництво, спрямоване на вивчення можливих шляхів зміцнення існуючих і розробку нових пропозицій щодо національних і міжнародних правових або інших заходів боротьби з кіберзлочинністю (ст. 9) [51].

Перше засідання Міжурядової групи експертів, що відбулося у Відні у 2011 році, розглянуло та затвердило обсяг і методологію дослідження. Питання, які мають бути розглянуті в рамках комплексного дослідження проблем кіберзлочинності, включають: питання кіберзлочинності, правові заходи боротьби з кіберзлочинністю, запобігання злочинності, варіанти кримінального правосуддя, інші заходи боротьби зі злочинами у сфері інформаційних технологій, діяльність міжнародних організацій у цій сфері та технічну допомогу. Слід зазначити, що для належного виконання поставленого перед нею завдання Міжурядова група експертів плідно співпрацює з Управлінням ООН з наркотиків і злочинності. Результати роботи експертної групи містяться в її звіті (наприклад, UNODC/CCPCJ/EG.4/2013/2).

15 січня 2015 року Генеральна Асамблея прийняла резолюцію A/RES/69/204 про використання ІКТ для розвитку, яка підкреслила позитивний імпульс у збільшенні доступності технологій ІКТ та фінансування, зокрема постійного розширення доступу до Інтернету, мобільного зв'язку, швидкого поширення комунікаційних з'єднань і

розгортання нових послуг і програм. Водночас, комісія стурбована великою невідповідністю між розвиненими країнами та країнами, що розвиваються, щодо охоплення широкосмуговим зв'язком, гендерної невідповідності в доступі до ІКТ та питань, які створюють несприятливі економічні умови для інвестиційної діяльності [52].

У резолюції A/RES/70/237 від 2015 року Генеральна Асамблея закликала держави-члени сприяти багатосторонньому розгляду існуючих і потенційних загроз інформаційній безпеці та можливих стратегій у цій сфері, якщо необхідно, для підтримки вільного потоку інформації; продовжувати вивчати відповідну міжнародну концепцію, спрямовану на підвищення безпеки глобальних інформаційних і телекомунікаційних систем [53].

Підсумовуючи, слід підкреслити, що Генеральна Асамблея ООН є представницьким дорадчим органом ООН, до повноважень якого входить обговорення нагальних питань, що зачіпають інтереси держав-членів та інших країн, одним із яких є боротьба з кіберзлочинністю. Під його егідою прийнято низку законопроектів, які містять положення щодо: регулювання інформаційного простору; захисту інформаційної інфраструктури; забезпечення безпеки користувачів Інтернет-сервісів; дотримання культури кібербезпеки; співпраці країн у боротьбі з кіберзлочинністю, в т.ч. обмін інформацією, правоохоронна професійна підготовка персоналу, забезпечення конфіденційності, цілісності та доступності даних комп'ютерної системи від несанкціонованого втручання тощо. Вона є ініціатором створення спеціалізованої групи експертів для вивчення питань у сфері боротьби з кіберзлочинністю, спеціалізованих установ ООН, які координують протидію кіберзлочинам (Управління ООН з наркотиків і злочинності, Конференція ООН з торгівлі і розвитку, Міжнародний союз електрозв'язку, Організація Об'єднаних Націй з питань освіти, науки і культури, Конференція ООН з торгівлі і розвитку тощо).

2.2. Інституційний механізм співробітництва держав щодо протидії злочинам у сфері інформаційних технологій в рамках Європейського Союзу

Європейський Союз (далі - ЄС) приділяє пильну увагу питанням протидії злочинам у сфері інформаійних технологій, підвищенню стійкості кіберсистем Союзу та іншим аспектам забезпечення кібербезпеки. Згідно зі статистичними даними, 1 млн осіб щодня стають жертвами правопорушень в Інтернеті [54].

Традиційно зазначені питання розглядаються в контексті взаємодії держав – членів ЄС у рамках простору свободи, безпеки та правосуддя [55].

Слід зазначити, що правовою основою регулювання співробітництва держав-членів ЄС у боротьбі з кіберзлочинністю є первинне право ЄС (установчі договори) та вторинне право ЄС (регламенти, директиви, рішення).

В установчих договорах ЄС передбачаються загальні засади взаємодії держав-членів ЄС у кримінально-правовій сфері. Вперше питання гармонізації кримінального законодавства, що регулює протидію кіберзлочинності, були включені до проекту Конституції для ЄС (ст. III-271) [56]. Надалі це положення також було закріплено і у Лісабонському договорі про внесення змін до Договіру про ЄС та Договору про заснування Європейського співтовариства від 13 грудня 2007 р. (далі – Лісабонський договір). У ст. 83 Договору про функціонування ЄС прямо вказується на право Ради ЄС та Європарламенту приймати нормативно-правові акти прямої дії, обов'язкові до виконання держав-учасниць ЄС [57].

Тим часом відсутність спеціальних норм, присвячених проблемі, не означає, що до набрання чинності Лісабонським договором протидія кіберзлочинності не регулювалася первинним правом ЄС. Так, нормативно-правовим інструментом гармонізації кримінального законодавства країн ЄС

на той період виступали рамкові рішення, які приймає Рада ЄС (наприклад, Рамкове рішення Ради 2005/222 про атаки на інформаційні системи).

В даний час детальне регулювання взаємодії держав у боротьбі з кіберзлочинністю здійснюється за допомогою актів вторинного права.

З метою гармонізації кримінального законодавства країн ЄС Радою ЄС було прийнято: Рамкове рішення від 22 травня 2001 р. щодо боротьби з шахрайством та підробкою безготівкових платіжних коштів, а також Директива Європейського Парламенту та Ради від 13 грудня 2011 р. про боротьбу з сексуальним насильством і сексуальною експлуатацією дітей та дитячою порнографією, та замінююча Рамкове рішення Ради 2004/68, Директива Європейського Парламенту та Ради від 12 серпня 2013 р. про атаки на інформаційні системи та замінююча Рамкове рішення Ради 2005/2.

Директива про атаки на інформаційні системи від 12 серпня 2013 р. криміналізує незаконний доступ до інформаційної системи, незаконне втручання в роботу системи, незаконний вплив на дані та незаконне перехоплення, протизаконне використання пристроїв та програмних засобів, у тому числі для створення ботнетів [55].

У тому випадку, коли незаконний вплив на комп'ютерні дані або системи пов'язаний з неправомірним використанням персональних даних іншої людини це може, відповідно до національного законодавства, вважатися обтяжливою обставиною, якщо такі дії не охоплюються нормами, що закріплюють інші злочини [56]. Крім того, директива збільшує розмір кримінальних покарань за скоєння кіберзлочинів.

Водночас, Директивою від 12 серпня 2013 р. не охоплюється низка злочинних діянь, які можуть відбуватися у глобальній інформаційній мережі Інтернет. Наприклад, питання гармонізації кримінального законодавства у сфері інтелектуальної власності поки що залишаються не врегульованими у праві ЄС [57].

Отже, питання зближення національного кримінального права у сфері протидії правопорушенням у сфері інтелектуальної власності в Інтернеті

поки не стало предметом правового регулювання в рамках ЄС. Крім того, у Директиві від 12 серпня 2013 р. не порушуються питання гармонізації кримінально-процесуального права. Більше того, цим актом не регламентується порядок здійснення міжнародного співробітництва з правоохоронними органами інших держав з метою боротьби зі злочинами у сфері інформаційних технологій.

Рамкове рішення від 22 травня 2001 р. щодо боротьби з шахрайством та підробкою безготівкових платіжних засобів містить норми, що передбачають необхідність включення до національного законодавства злочинів, що стосуються: платіжних документів, комп'ютерів та спеціально пристосованих пристроїв (ст. 2–4) [53].

У зв'язку з появою нових способів здійснення шахрайства та підробки безготівкових платіжних коштів у план законопроектної діяльності Єврокомісії на 2016 р. було включено пункт про розробку проекту Директиви, яка б криміналізувала суспільно небезпечні діяння, що здійснюються в процесі проведення онлайн платежів, а також враховувала б новітні тенденції у способах та засобах здійснення шахрайства з використанням комп'ютерної техніки (наприклад, скімінг, фішинг та фармінг). Наразі Єврокомісією підготовлено проект відповідного нормативного правового акту, але поки що його не було прийнято Європейським Парламентом та Радою [45].

Директива Європейського Парламенту та Ради від 13 грудня 2011 р. про боротьбу із сексуальним насильством та сексуальною експлуатацією дітей та дитячою порнографією, що заміняє Рамкове рішення Ради 2004/68 криміналізувала цілу низку діянь, деякі з яких можуть здійснюватися через Інтернет (ст. 5 «Злочини, що стосуються дитячої порнографії», ст. 6 «Пристава́ння до дітей із сексуальною метою» (в тому числі через Інтернет). Незважаючи на те, що розглянута вище Директива була прийнята у 2011 р., її зміст, як і раніше, не втратив своєї актуальності. Так, у резолюції Європарламенту від 11 березня 2015 р. наголошується на важливості

виконання вищезгаданого документа всіма державами-членами ЄС, а також вказується на необхідність використання ширшого за змістом терміну «матеріал про сексуальне насильство над дітьми», замість «дитяча порнографія» [59].

Правовою основою гармонізації кримінального законодавства держав-членів ЄС у боротьбі з тероризмом наразі є Директива Європейського парламенту та Ради 2017/541 про боротьбу з тероризмом від 15 березня 2017 року [60]. У цьому документі немає спеціальних норм, присвячених кібертероризму. Це обумовлено дискусійністю самого терміну «кібертероризм», і питанняv необхідності включення такого складу злочину до законодавства [59]. У той же час у розглянутій директиві передбачені окремі положення, спрямовані на попередження використання глобальної мережі Інтернет з терористичною метою: публічне підбурювання до скоєння терористичного злочину (ст. 5), заходи проти провокаційного контенту в Інтернеті (ст. 21). Крім того, вважаємо, що незважаючи на те, що у зазначених вище нормах, немає прямих посилань до заборони використання Інтернету з терористичною метою, така діяльність охоплюється змістом ст. 5, 7, 8 цієї Директиви.

Співпраця правоохоронних органів у рамках запобігання та розслідування кібер-злочинів будується на основі Конвенції ЄС про взаємну правову допомогу щодо кримінальних справ між державами-членами ЄС від 29 травня 2000 року [55].

Окремі аспекти взаємодії держав-членів ЄС у боротьбі з кіберзлочинністю конкретизовано у рекомендаційних актах інститутів ЄС (передача персональних даних, приєднання до мережі контактних пунктів 24/7, використання таких інструментів як європейський ордер на арешт та європейський ордер на провезення) розслідування у кримінальних справах)[61].

Так, відповідно до Рамкового рішення Ради від 13 червня 2002 р. «Про європейський ордер на арешт та процедуру видачі між державами-членами

ЄС» (із змінами, внесеними Рамковим Рішенням Ради від 28 березня 2009 р.) щодо злочинів, пов'язаних з інформаційними технологіями, не потрібна перевірка подвійної криміналізації діяння, якщо вона карається позбавленням волі або ув'язненням не менше ніж три роки, а також, якщо стосовно них може застосовуватися процедура видачі відповідно до закону.

Використання такого інструменту як «європейський ордер на арешт» суттєво спрощує міжнародне співробітництво між державами-членами ЄС у сфері боротьби з кіберзлочинністю, оскільки він: а) видається безпосередньо судовим органом держави, яка запитує; б) виконується безпосередньо судовим органом запитуваної держави [62].

На підставі Директиви про європейський ордер на проведення розслідування від 3 квітня 2014 р. злочини, пов'язані з комп'ютерами, входять до переліку діянь, щодо яких не потрібна перевірка подвійної криміналізації, якщо вони караються позбавленням волі або ув'язненням не менше трьох років у державі виконання ордера для проведення розслідування [61]. Це означає, що на підставі ордера, виданого або затвердженого судом держави, що запитує, у запитуваній державі можуть проводитися слідчі дії для отримання доказів у кримінальній справі, порушеній у зв'язку з вчиненням кіберзлочину.

Слід зазначити, що міжнародну координацію співробітництва держав-членів ЄС у боротьбі з тяжкими кіберзлочинами, що зачіпають територію двох або більше держав – членів ЄС, здійснюють спеціально створені на загальноєвропейському рівні органи: Європол та Євроюст (ст. 85, 88) [63].

Відповідно до підпункту b п. 1 ст. 88 Договору про функціонування ЄС Європол може здійснювати координацію, організацію та здійснення розслідувань та оперативно-розшукових заходів, що проводяться спільно з компетентними органами держав-членів або в рамках спільних слідчих груп, за потреби у взаємодії з Євроюстом. Для цих цілей у структурі Європолу було створено Європейський центр кіберзлочинності.

Відповідно до ст. 85 Договору про функціонування ЄС призначенням Євроюсту є підтримка та посилення координації та співпраці національних органів, відповідальних за проведення розслідувань та кримінального переслідування за фактами тяжкої злочинності, яка торкається двох або більше держав-членів або вимагає проведення кримінального переслідування загальних засадах – з операцій, здійснюваних органами держав-членів і Європолом, на основі наданої ними інформації. Євроюст у межах своєї компетенції проводить спеціальні наради щодо боротьби з кіберзлочинністю, координує створення спільних слідчих груп для розслідування таких злочинів[64].

Таким чином, у ЄС використовується системний підхід для координації співробітництва держав – членів ЄС у боротьбі з кіберзлочинністю, який включає регулювання основ такої взаємодії в установчих договорах ЄС та відповідно до їх положень – детальну регламентацію такої співпраці у регламентах та директивах Європейського Парламенту та Ради.

В даний час у праві ЄС містяться положення, спрямовані на гармонізацію законодавства держав-членів ЄС у сфері, що розглядається, а також передбачаєть спрощений порядок взаємодії компетентних органів держав – членів ЄС з метою припинення, розслідування кіберзлочинів та залучення до кримінальної відповідальності осіб, які їх вчинили. Крім того, ефективна координація проведення спільних оперативно-розшукових заходів та слідчих дій здійснюється спеціально створеними на рівні ЄС відомствами – Європолом та Євроюстом.

Разом з тим, вважаємо, що тяжкі кіберзлочини можуть припускати не лише використання всіх розглянутих вище заходів кримінально-правового характеру, а й задіяння інституційних механізмів боротьби з кіберзлочинами, регламентованими ЄС у рамках спільної зовнішньої та безпекової політики.

Слід зазначити, що думка щодо можливості відповіді на кіберінциденти за допомогою інструментів загальної політики безпеки та оборони також містилася у рекомендаційному акті Європейського парламенту – Резолюції

2012/2223 (INI) «Положення про взаємну оборону та солідарність ЄС: політичні та оперативні аспекти» [65]. Безумовно, не будь-який інцидент з використанням інформаційних технологій можна кваліфікувати як кіберзлочин. Так, до кіберинцидентів належать будь-які кібератаки, незалежно від суб'єкта, який їх вчинив, та незалежно від їх конкретних наслідків. З іншого боку, термін «кібер інцидент» є досить широким за своїм значенням, і включає кіберзлочини.

Відповідно до ст. 222 Договору про функціонування ЄС Союз і держави-члени ЄС діють спільно в дусі солідарності, якщо одна з держав-членів стає жертвою, у тому числі катастрофи, спричиненої людиною. При цьому Союз може мобілізувати всі наявні у нього інструменти, у тому числі надані у його розпорядження державами-членами військові кошти. Відповідно до п. 3 ст. 222 цього договору «порядок реалізації Союзом цієї умови солідарності визначається рішенням, прийнятим Радою за спільною пропозицією Комісії та Верховного представника Союзу із закордонних справ та політики безпеки. Коли таке рішення має наслідки у сфері оборони, Рада ухвалює відповідно до п. 1 ст. 31 Договору про Європейський Союз та інформує Європейський парламент [56].

Відповідно до п. а ст. 3 Рішення Ради від 24 червня 2014 р. щодо заходів здійснення Союзом застереження про солідарність, під терміном «катастрофа» розуміється «будь-яка ситуація, яка має чи може серйозно впливати на людей, довкілля чи власність, включаючи культурний спадок» [56]. При формулюванні даного визначення ключовим став акцент на характері шкоди, яка може бути завдана внаслідок інциденту; у ньому не вказується на потенційного суб'єкта заподіяння шкоди. Отже, поняття «катастрофа, викликана людиною» є дуже широким і може включати як дії, вчинені приватними особами, так і акти, які можуть бути атрибовані державі.

Водночас, як було зазначено під час дискусій у Європарламенті про правову природу та механізм реалізації ст. 222 Договору про функціонування ЄС, застереження про солідарність може використовуватися у відповідь не на

звичайну кризу (повені, лісові пожежі), а на виняткові ситуації, коли не вистачає ні можливостей постраждалої держави, ні традиційних кризових механізмів ЄС для врегулювання проблеми. Зазначена криза, як правило, має транскордонний та трансекторальний характер [56].

Порядок вирішення питання щодо доцільності залучення ст. 222 Договору про функціонування ЄС роз'яснюється у п. 3.2 Європейської стратегії про кібербезпеку «Відкритий, безпечний та чесний кіберпростір» від 7 лютого 2017 року [66]. Цей документ не є нормативним правовим актом і окреслює загальні політичні засади забезпечення кібербезпеки.

У Європейській стратегії про кібербезпеку визначено порядок реагування на різні типи кіберінцидентів. Так, відповідно до п. 3.2 вказаного акта, якщо кіберінцидент є злочином, про це повідомляється Європол та Європейський центр кіберзлочинності з тим, щоб вони могли спільно з компетентними органами держав-членів ЄС відреагувати на нього [32]. Водночас держава-член ЄС может апелювати до ст. 222 Договора про функціонування ЄС у випадку, якщо інцидент: а) відноситься до кібершпигунства або атаки, спонсорованої державою, або має наслідки для національної безпеки; б) є особливо серйозним. У документі не пояснюється, що являє собою «особливо серйозний інцидент», що ускладнює можливість застосування цих критеріїв.

З огляду на той факт, що тлумачення ст. 222 Договору про функціонування договору про ЄС, який міститься в Стратегії про кібербезпеку, не обмежує особливо серйозні інциденти лише діями, які вжито державними акторами, вжиття спільних заходів у відповідь на особливо небезпечний кіберзлочин не суперечитиме праву ЄС.

У той же час, слід зазначити, що можливість застосування збройних сил у відповідь злочин у сфері інформаційних технологій є практично неможливим. Але навіть і в цьому випадку метою такої малоймовірної операції стане саме нейтралізація усунення наслідків широкомасштабного та

руйнівного злочину у сфері високих технологій, а не застосування сили в сенсі ст. 51 Статуту ООН.

Слід зазначити, що реалізація ст. 222 Договору про функціонування ЄС можливе лише відповідно до принципу комплементарності та узгодженості дій держав-членів та Союзу.

У резолюції Європейського парламенту 2012/2223 (INI) «Положення про взаємну оборону та солідарність ЄС: політичні та оперативні аспекти» зазначається, що «застереження про солідарність слід застосовувати в ситуаціях, в яких потенціал реагування постраждалої держави-члена перевищено або якщо ситуація вимагає вжиття багатопрофільних заходів у відповідь за участю різних суб'єктів» [56]. Таким чином, застереження про солідарність може застосовуватися щодо кіберинцидентів, щодо яких держава-член ЄС: а) вичерпав усі внутрішні можливості щодо реагування на нього; б) не в змозі самостійно вжити заходів, достатніх для відповіді на цей кіберінцидент.

Враховуючи вище викладене можна дійти наступних висновків.

ЄС використовується системний підхід для координації співробітництва держав-членів ЄС у боротьбі зі злочинами у сфері інформаційних технологій, який має правовий та інституційний компонент. Виявлено, що специфіка змісту актів вторинного права, що регулюють співпрацю держав-членів ЄС у боротьбі з кіберзлочинністю полягає в тому, що вони: а) спрямовані на гармонізацію кримінального законодавства у даній сфері; б) регламентують міжнародне співробітництво у боротьбі з такими злочинами; в) встановлюють спрощений порядок оперативної взаємодії компетентних органів за рахунок використання таких інструментів як європейський ордер на проведення розслідування, європейський ордер на арешт.

Водночас нині в ЄС відсутня правова основа для гармонізації кримінального законодавства держав-членів ЄС у боротьбі з кіберзлочинами у сфері інтелектуальної власності; потребує перегляду Рамкове рішення від 22 травня 2001 р. щодо боротьби з шахрайством та підробкою безготівкових

платіжних коштів. Все це свідчить про необхідність подальшого вдосконалення правового регулювання співпраці у боротьбі з кіберзлочинністю в рамках ЄС.

У відповідь на окремі кіберзлочини ЄС держави можуть клопотати про застосування заходів, передбачених ст. 222 Договору про функціонування ЄС, що включають, зокрема, використання військового потенціалу держав-членів ЄС. При цьому такі кіберзлочини мають: а) бути особливо серйозними та загрожувати національній безпеці держав-членів ЄС; б) мати транскордонний, транссекторальний та широкомасштабний характер; в) вимагати вживання багатопрофільних заходів у відповідь за участю різних суб'єктів у ситуації, коли потерпіла держава не має достатнього потенціалу для реагування на такі інциденти.

2.3. Інституційні механізми поліцейського співробітництва щодо протидії злочинам у сфері інформаційних технологій

Суспільно-небезпечні дії у сфері інформаційно-комунікаційних технологій, які називаються в юридичній літературі кіберзлочинами, є глобальною транснаціональною загрозою для світової спільноти. На жаль, вирішити цю проблему на рівні окремих країн неможливо, тому що специфіка цього виду злочину передбачає вчинення їх в іншому, віртуальному кіберпросторі, який не визнає кордонів держав.

У зв'язку з цим актуальною проблемою стало підвищення ефективності методики розкриття та розслідування злочинів у сфері інформаційних технологій. У цьому плані важливе значення має міжнародне співробітництво (взаємодія) правоохоронних органів. Основним міжнародним координуючим, організаційним структурним підрозділом, що забезпечує ефективність у сфері міжнародної взаємодії, у розробці оптимальної методики правозастосовчої діяльності національних

правоохоронних органів є Інтерпол (Міжнародна організація кримінальної поліції (далі - Інтерпол). Основним завданням Інтерполу є об'єднання зусиль національних правоохоронних органів країн-учасниць (194 держави) у сфері боротьби із загальнокримінальною злочинністю[67].

Актуальність боротьби з кіберзлочинами обумовлена тим, що транснаціональний характер вимагає узгоджених міжнародних зусиль боротьби з ними. В умовах постійного вдосконалення методів та засобів скоєння кіберзлочинів зростає значення діяльності Інтерполу як універсальної міжнародної організації, яка здійснює координацію співробітництва держав у сфері, що розглядається. У зв'язку з цим необхідно визначити, які заходи, вживаються Інтерполом для забезпечення ефективної співпраці у боротьбі зі злочинами у сфері інформаційних технологій, є найефективнішими.

Різний рівень науково-технічного розвитку, інформаційно-комунікаційних технологій, необхідної нормативно-правової бази в галузі, що розглядається, ускладнюють процес співробітництва країн у протидії кіберзлочинності [68].

У кожній державі-учасниці цієї міжнародної організації кримінальної поліції утворено Національні центральні бюро Інтерполу (НЦБ) [69]. Не стала винятком і Україна [70], де створено необхідні умови для міжнародного співробітництва у протидії кіберзлочинності. Постановою Кабінету Міністрів України від 25 березня 1993 року № 220 затверджено нову редакцію Положення про Національне центральне бюро Інтерполу в Україні, в якому доповнено положення про дієві методи розслідування кіберзлочинів.

Для правильного розуміння кіберзлочинів як транснаціонального різновиду міжнародної злочинності слід усвідомити, що розуміється під цими суспільно-небезпечними діяннями, однак єдиної думки щодо цих визначень науковцям так і не вдалося досягти, про що ми уже повідомляли раніше.

Інтерпол кожної держави є координуючим органом міжнародного співробітництва правоохоронних органів країн-учасниць у сфері боротьби зи злочинами з використанням інформаційних технологій [69], а щодо кримінально-правового регулювання кіберзлочинів, то першою ініціативою, вжитою Інтерполом у контексті міжнародно-правового врегулювання проблеми кіберзлочинності, була Паризька конференція 1979 року. Вперше, у пропозиціях конференції, у її підсумковому документі знайшли своє відображення положення про необхідність міжнародно-правового регулювання кіберзлочинів як різновиду транснаціональної злочинності [72].

Діяльність Інтерполу щодо координації співробітництва країн визначає алгоритм міжнародної взаємодії у боротьбі з кіберзлочинами. Механізм скоєння цих суспільно-небезпечних діянь має міжнародно-правовий, транснаціональний характер, а тому для розробки приватної криміналістичної методики їх розкриття та розслідування необхідно визначити основні критерії міжнародного співробітництва. Слід визнати, що Інтерпол був першою міжнародною організацією, яка спробувала співвіднести злочини до сфери інформаційних технологій та міжнародне кримінальне, кримінально-процесуальне право, оперативно-розшукову транснаціональну діяльність та особливості відповідного національного законодавства країн-учасниць Інтерполу.

Інтерпол систематично, цілеспрямовано проводить моніторинг та огляд практики скоєних кіберзлочинів та нормативно-правовий аналіз чинного законодавства країн-учасниць у протидії кіберзлочинності. Це відноситься і до всесвітньої глобальної мережі, де особливе місце займає Інтернет, за допомогою якого у віртуальному просторі і скоюються кіберзлочини [73].

Наступним етапом становлення регулювання механізму співробітництва у боротьбі з кіберзлочинністю стала, проведена у квітні 1995 року, I Міжнародна конференція Інтерполу з комп'ютерної злочинності. У роботі конференції взяли участь 49 країн, а також представник Ради Європи як спостерігач. Крім представників правоохоронних органів до складу делегацій

входили співробітники спецслужб, служб безпеки банків, фахівці та експерти у галузі інформатики [74].

Співробітництво у боротьбі з кіберзлочинами Інтерпол здійснює за допомогою обміну інформацією, що допомагає у розкритті цих злочинів, та цей обмін має міжнародно-правовий характер. Необхідно визнати інформаційно-забезпечуючу роль Інтерполу у протидії цим злочинам. При розслідуванні кіберзлочинів правоохоронні органи можуть отримати зі спеціалізованої закритої автоматизованої системи відомості про провайдерів та дистриб'юторів мережевих та телекомунікаційних послуг, мережеві адреси, імена доменів та серверів, та іншу необхідну інформацію [72].

Діяльність Інтерполу щодо координації міжнародного співробітництва держав у протидії кіберзлочинності здійснюється його спеціалізованими органами, серед яких основними центральними органами управління є Генеральна Асамблея (вищий пленарний орган Інтерполу) та Виконавчий комітет (вищий адміністративно-виконавчий орган). Відповідно до статті 25 Статуту постійно діючим органом Інтерполу є Генеральний секретаріат, який проводить у життя рішення Генеральної Асамблеї та Виконавчого комітету.

По суті, Інтерпол виступає як міжнародний центр боротьби зі злочинністю і діє як спеціалізований та інформаційний центр, який здійснює ефективне керівництво його діяльністю. Ця організація підтримує контакти з національними правоохоронними та міжнародними органами та видає матеріали, які можуть бути доцільними та ін. [69].

Слід наголосити, що Національні центральні бюро (НЦБ) є постійно діючими правоохоронними структурними підрозділами Інтерполу в окремо взятій країні та наділені широкими повноваженнями щодо координації боротьби зі злочинами у сфері інформаційних технологій. Саме вони є необхідними посередницькими органами, які виступають ланками міжнародного співробітництва держав у боротьбі з кіберзлочинністю. Реалізація координуючого механізму здійснюється шляхом безпосереднього співробітництва через контакти НЦБ країни та Генерального секретаріату

Інтерполу. Особливістю посередницьких процесів НЦБ і те, що вказівки, які від даної міжнародної організації, мають рекомендаційний характер [75].

НЦБ Інтерполу в Україні входить до структурного підрозділу МВС на правах самостійного оперативного управління, основним завданням якого є забезпечення співпраці з правоохоронними органами інших держав-учасниць Інтерполу у розкритті та розслідуванні кіберзлочинів.

Як зазначалося, кіберзлочини відбуваються за допомогою різних інформаційно-комунікаційних технологій, і навіть інших інформаційних засобів у специфічному інформаційному віртуальному просторі і мають транснаціональний, міжнародний характер. Отже, саме Інтерпол створює умови для одноманітного розуміння та застосування приватної криміналістичної методики розслідування кіберзлочинів. І тому необхідно створити механізм глобальної гармонізації нормативно-правового регулювання боротьби з кіберзлочинністю.

По суті, основна координуюча діяльність Інтерполу у протидії кіберзлочинності виявляється у нормативно-правовому регулюванні спільних дій держав для ефективної взаємодії. Генеральною Асамблеєю Інтерполу прийнято окремі резолюції, які безпосередньо належать до методики розслідування кіберзлочинів. До них можна віднести резолюцію, прийняту за підсумками 6-ї Міжнародної конференції з кіберзлочинності, що відбулася в Каїрі, яка рекомендує країнам-учасницям приєднатися до Конвенції про кіберзлочинність як до документу, що закріплює мінімальні стандарти у сфері боротьби з кіберзлочинністю. Пріоритетним напрямом організаційного характеру механізму співробітництва було визначено завдання щодо підготовки кадрів у боротьбі з кіберзлочинністю за допомогою розвитку відповідних навчальних курсів та створення міжнародної мережі навчальних інститутів, що включають оптимальне використання інструментів та програм, таких як Мобільний кабінет Інтерполу та модулі електронного навчання. При цьому визначалося, що інформація щодо кримінальних справ у сфері інформаційних технологій, має накопичуватися в базі даних

Інтерполу та поширюватися у формі аналітичних продуктів, щоб допомогти державам-членам у прийнятті відповідних стратегій запобігання цьому виду злочинів[76].

На підставі вищевикладеного можна зробити висновок про те, що діяльність Інтерполу з координації міжнародно-правового співробітництва у боротьбі з кіберзлочинністю здійснюється у таких основних напрямках: у міжнародній координації діяльності правоохоронних органів окремих держав на національному рівні шляхом розробки єдиних рекомендацій щодо методики розкриття та розслідування кіберзлочинів; у створенні спеціальних координуючих підрозділів у структурі Інтерполу, відповідальних за реалізацію оптимальної співпраці для боротьби зі злочинами у сфері інформаційних технологій; у розробці та здійсненні спільних програм практичної діяльності з протидії кіберзлочинності; у розробці та прийнятті інституційних засад діяльності Інтерполу за методикою боротьби з кіберзлочинністю; у прийнятті «Дорожньої карти» щодо здійснення необхідних заходів щодо обміну досвідом та навчання співробітників правоохоронних органів держав-учасниць, а також у підготовці методики розкриття та розслідування злочинів у сфері інформаційних технологій.

Таким чином, діяльність Інтерполу у сфері боротьби з кіберзлочинністю здійснюється шляхом реалізації правотворчих, інституційних та організаційних заходів.

РОЗДІЛ 3. ТЕНДЕНЦІЇ МІЖНАРОДНО-ПРАВОВОГО СПІВРОБІТНИЦТВА ДЕРЖАВ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

3.1. Перспективи вдосконалення механізмів міжнародно-правового співробітництва держав щодо протидії злочинам у сфері інформаційних технологій

Прискорення розвитку інформаційного суспільства надає країнам величезні переваги в багатьох сферах суспільного життя. Проте створення нових можливостей для подальшого розвитку та використання інформаційних технологій неминуче призводить до виникнення відповідних проблем в інформаційному полі. Однією з таких проблем, яка в останні роки все більше глобалізується, є злочинність у сфері інформаційно-комунікаційних технологій (ІКТ). Це явище зростає не лише на локальному, а й на глобальному рівнях і вже створило загрозу для всієї міжнародної системи інформаційної безпеки.

Поява, масштаби та складність таких транснаціональних комп'ютерних злочинів чітко показують, що жодна країна не може їх побороти у повній мірі, покладаючись лише на власні сили. Тому потрібна міжнародна співпраця у цьому напрямку має пріоритетне значення [77].

Аналіз стратегії міжнародного співробітництва у сфері протидії кіберзлочинності на сучасному етапі показує, що концепції, теорії та методи застосування міжнародних організацій для здійснення міжнародного співробітництва у цій сфері мають як спільні, так і відмінні риси, які зумовлені різними поглядами про пріоритети в цій сфері. Інформаційна безпека країн-учасниць цих інституцій, у свою чергу, пов'язана з різними рівнями їх інформаційного розвитку.

Прийняті з цього приводу міжнародні документи можна умовно поділити на такі: 1) визнають наявність проблеми та закликають до боротьби з цими злочинами; 2) закладають основу для співпраці проти кіберзлочинності та/або передбачають окремі види міжнародної злочинності в секторі ІКТ 3) створюють інституції, спрямовані на вжиття заходів для боротьби з такими злочинами, або створення платформ для співпраці у цій сфері (конференції, форуми тощо).

Згадана вище перша група міжнародно-правових актів в основному представляє так звані «soft low». Серед них особливо варто відзначити резолюцію Генеральної Асамблеї ООН, присвячену цьому питанню

(Резолюція Генеральної Асамблеї ООН «Боротьба зі злочинним використання інформаційних технологій»; від 4 грудня 2000 р., № 55/63, від 19 грудня 2001 р. №56/121) або розглядаючи її у контексті інформаційної безпеки (Декларація тисячоліття ООН 2000 р., Резолюції Генеральної Асамблеї ООН «Досягнення у сфері інформації та комунікації в контексті міжнародної безпеки» від 4 грудня 1998 року No 53/70, від 1 грудня 1999 року No 54/49, від 20 листопада 2000 року No 55/28, від 29 листопада 2001 року No 56/19, від 22 листопада 2002 року No 57/53, від 8 грудня 2003 року No 58/32, від 3 грудня 2004 року No 59/61, від 8 грудня 2005 року No 60/45, від 6 грудня 2006 року No 61/54, від 5 грудня 2007 року No 62/17, від 2 грудня 2008 року No 63/37, від 2 грудня 2009 року No 64/25, від 8 грудня 2010 року No 65/41, від 13 грудня 2011 року No 66/24, Резолюція Генеральної Асамблеї Організації Об'єднаних Націй «Заходи з ліквідації міжнародного тероризму» 2003 р. №56/27, Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки і захист найважливі- ших інформаційних структур» від 20 грудня 2002 року No57/239, від 23 грудня 2003 року No 58/199, від 21 грудня 2009 року No 64/211, Декларація принципів «Побудова Інформаційного суспільства — глобальне завдання в новому тисячолітті» 2003 р. тощо). Економічна і Соціальна Рада ООН ратифікувала Резолюції «Міжнародне співробітництво у справі щодо попередження і розслідування шахрайства, злочинного неправомірного використання і фальсифікації особистих даних і пов'язаних з ними зло- чинів, а також переслідування та покарання за них» від 21 липня 2004 року No 2004/26, від 26 липня 2007 року No 2007/20.

Міжнародний союз електрозв'язку також дуже серйозно ставиться до боротьби зі злочинами у сфері інформаційних технологій. Дії групи визнають існування проблем кіберзлочинності та закликають до боротьби з ними, включаючи Резолюцію 71 «Стратегічний план Коаліції на 2016-2019 рр.», Резолюцію 130 «Підвищення ролі ITU у зміцненні довіри та безпеки під час використання інформаційно-комунікаційних технологій», Резолюцію 174

«Роль ITU в питаннях міжнародної публічної політики, пов’язаної із ризиком незаконного використання інформаційно-комунікаційні технології», Резолюцію 181 (Гвадалахара, 2010) «Визначення та термінологія, що стосуються підвищення довіри та безпеки при використанні інформаційно-комунікаційних технологій» тощо [78].

Діяльність Організації економічного співробітництва та розвитку (далі - ОЕСР) у сфері боротьби з кіберзлочинністю в основному спрямована на проведення досліджень щодо можливості гармонізації кримінального законодавства в цій сфері. У 1992 році Рада ОЕСР прийняла рекомендації з інформаційної безпеки. Цей документ передбачає, що країни приймають національні правила для забезпечення цілісності та конфіденційності інформаційних систем та інформації, що в них обробляється, шляхом прийняття складних організаційних і технічних заходів безпеки. У 2002 році Рада ОЕСР рекомендувала нову версію Принципів «Рекомендації ОЕСР щодо безпеки інформаційних систем і мереж: на шляху до культури безпеки». Ці документи є мінімальним стандартом для консенсусу між країнами-членами ОЕСР [79].

У Європейському Союзі питання забезпечення безпеки у інформаційному просторі зосереджені насамперед на захисті цілісності інформації та інформаційних систем, забезпеченні належних умов для їх обігу та цінності. Серед нормативних актів у цій сфері можна назвати, зокрема, Резолюцію 2007 року про Стратегію європейського інформаційного суспільства (Résolution du Conseil du 22 mars 2007 relative á un strategy pour une société de l'information sûre en Europe), січень 1999 року; Рішення від 25 червня 2016 року №. 276/1999/ЕС про багаторічний план дій спільноти для сприяння безпечному використанню Інтернету шляхом боротьби з незаконним і шкідливим вмістом у глобальній мережі (план «Безпечніший Інтернет» (1999-2004), «Безпечний Інтернет Плюс» (2005-2008), «Безпечний Інтернет 2009-2013», спільне повідомлення з Європейським парламентом,

Європейською радою, Європейським економічно-соціальним комітетом і Комітетом регіонів «Перегляд Європейської політики сусідства» 2015 р. [80].

Крім того, в рамках ЄС прийнято низку програм щодо боротьби з кіберзлочинністю, зокрема: «Електронна Європа», «План дій в Інтернеті», «Технології інформаційного суспільства». Програма ЄС «Запобігання та боротьба зі злочинністю» передбачає фокус співпраці у сфері боротьби з кіберзлочинністю [81].

Важливим внеском Шанхайської організації співробітництва (далі – ШОС) у створенні основи міжнародного співробітництва є документ під назвою «Конвенція про забезпечення міжнародної інформаційної безпеки» [82], який був запропонований для обговорення під час 66-ї сесії Генеральної Асамблеї ООН. Основна мета документа – визначити права та обов'язки держав в інформаційному просторі, спонукати їх до відповідальної поведінки та активізувати співпрацю, в тому числі у боротьбі з комп'ютерною злочинністю. Законопроект так і не був прийнятий.

Усі перераховані вище документи, хоча більшість із них є рекомендативними, створюють основу для подальшої співпраці між країнами для вирішення теоретичних і практичних питань у цій сфері на глобальному та регіональному рівнях.

Нормативно-правових актів другої категорії наразі небагато, оскільки визначити певні злочини як міжнародні злочини (міжнародні кримінальні правопорушення) та реалізувати комплексне багатостороннє співробітництво для боротьби з цими злочинами на практиці важко з багатьох причин.

Рамкове рішення ЄС «Про атаки на інформаційні системи» від 2005 року визначає три категорії відповідальності за навмисні злочини: 1) незаконний доступ до інформаційних систем; 2) порушення цілісності систем; 3) порушення конфіденційності даних. На відміну від вищезазначеного нормативного акту, який передбачає обов'язок самостійно визначати кримінальні санкції, Рамкове рішення вимагає від держав-членів встановити

конкретні строки позбавлення волі за останні дві категорії правопорушень[83].

Міжнародні документи закріплюють багато форм і рівнів співробітництва. Наприклад, Глобальний план кібербезпеки ITU 2007 року вбачає такі форми співпраці, за яких організовуються окремі структури, як спостереження, сповіщення та реагування на події, підготовка відповідних пропозицій, співпраця на рівні регіональних та глобальних конференцій [84].

Питання, не охоплені цими міжнародними правилами, вирішуються відповідно до конвенцій та угод про співпрацю у сфері правової допомоги, а також національного законодавства.

Відповідно до вищезазначеної третьої групи міжнародних актів, були створені кооперативні інституції та платформи з різними повноваженнями та цілями: від обговорення питань кіберзлочинності до реальних дій проти кіберзлочинності. Серед них варто згадати: ITU – регіональні зустрічі та група експертів високого рівня з кібербезпеки (HLEG) (згідно з Глобальним планом кібербезпеки, зобов'язання ITU 2007 року щодо забезпечення глобальної кібербезпеки, існуючих загроз безпеці, передбачення нових і майбутніх проблем, досягнення запланованих цілей тощо); CE – Комітет експертів з кіберзлочинності (згідно з рішенням CDPC/103/211196), Комітет експертів з кіберзлочинності (згідно з CM /Del/Dec(97)583); EU – Європейське агентство з мережевої та інформаційної безпеки (згідно з постановами Парламенту та Ради від 2004 року), Група швидкого реагування на комп'ютери (для допомоги в боротьбі з новітніми комп'ютерними вірусами, для розробки Інтернет-стратегії для Європейської Комісії), Європейський центр боротьби з кіберзлочинністю (створений у 2014 році відповідно до Стратегії внутрішньої безпеки ЄС 2011; забезпечує інформаційну, оперативну та експертну підтримку розслідувань на міжнародному та регіональному рівнях).

У 2006 році була створена Міжнародна організація у боротьбі з кібертероризмом «ІМПАКТ» (спільні представники держави та бізнесу для

пошуку та впровадження найбільш ефективних методів боротьби з кібертероризмом).

Юридична можливість виконання міжнародних заходів є лише одним із факторів їх фактичного впровадження. Дійсно, небагато випадків, коли країна була змушена впроваджувати міжнародні заходи всупереч власним інтересам безпеки чи всупереч волі свого уряду, своїх найпотужніших галузей промисловості чи сильної громадської думки. Безпека, політика, економіка та міжнародна репутація виявляються набагато більш визначальними факторами в цій перспективі [85].

По-перше, безпека є ключовим фактором, що визначає впровадження міжнародних заходів. Швидке ухвалення Рамкового рішення про Європейський ордер на арешт і Рамкового рішення про боротьбу з тероризмом можна вважати реакцією на атаки 11 вересня 2001 року. У цій перспективі міжнародні заходи щодо кіберзлочинності все більше пов’язані з національною безпекою, особливо щодо захисту національних інфраструктур.

По-друге, політика може вплинути на реалізацію політичних міжнародних заходів. Дуже добре відомі проблеми у прийнятті та реалізації міжнародних інструментів проти тероризму (принаймні до 2001 року). Міжнародні заходи щодо кіберзлочинності (за винятком криміналізації актів расизму та ксенофобії через комп’ютерні системи, передбачені Додатковим протоколом до Конвенції Ради Європи) видаються менш чутливими з політичної точки зору.

По-третє, національна економіка може впливати на реалізацію заходів, які можуть суттєво вплинути на окремі ринки. Труднощі в переговорах і ратифікації міжнародних правил запобігання зміні клімату та скорочення викидів є прикладом цього впливу. Міжнародні заходи проти кіберзлочинності впливають на бізнес інтернет-послуг провайдерів та інших операторів ринку, які запитують дані та інформацію для зберігання. Проте характеристики цих ринків можуть сприяти впровадженню міжнародних

стандартів. Дійсно, завдяки ІКТ компанії можуть отримати доступ до кількох національних ринків з більшою легкістю, ніж в інших, більш традиційних секторах (наприклад, автомобільна, харчова, металургійна). Дійсно, ІКТ надають можливість вийти на ринки в усьому світі. Наявність спільних правил і стандартів важлива для створення рівних умов і відкриття шляху до нових ринків.

По-четверте, міжнародна репутація може впливати на виконання заходів, які привертають увагу громадськості. Це стосується міжнародних угод, наприклад, щодо ядерної енергії, ядерної зброї, геноциду та військових злочинів. Країни, які не впроваджують ці заходи, піддаються стигматизації, і це негативно впливає на їхню міжнародну репутацію. Здається, що міжнародні заходи щодо протидії злочинам у сфері інформаційних технологій не мають подібного впливу на громадську думку.

Ці елементи сприяють кращому поясненню динаміки імплементації поточної європейської бази щодо злочинів у сфері інформаційних технологій. Самі по собі правові зобов'язання не дають достатнього пояснення поточного рівня виконання. Крім того, країни, які не мають юридичних зобов'язань щодо впровадження міжнародних заходів, приводять своє законодавство до цього. Фактори безпеки, політики, економіки та репутації є додатковими значущими змінними.

Отже, проведений аналіз показує, що існує нагальна потреба в розробці процедур і практичних механізмів боротьби з правопорушеннями у сфері інформаційних технологій в Україні. Впровадження нових процедур та нормативно- правових актів європейського напрацювання зможе усунути деяку неоднозначність у цій сфері. Цей крок також сприяє реформуванню української системи боротьби з кіберзлочинністю.

3.2. Пріоритетні напрями міжнародного співробітництва України у сфері забезпечення безпеки інформаційного простору

Україна є повноправним учасником глобальної системи безпеки, пріоритетами якої залишаються розвиток міжнародного партнерства та співробітництва у сфері боротьби зі злочинами з використанням інформаційних технологій, підтримка міжнародних ініціатив у сфері кібербезпеки в національних інтересах, компетенції у сфері кібербезпеки, участь у діяльність зі зміцнення довіри в кіберпросторі тощо. Згідно з укладеними Україною міжнародними договорами, Україна проводить виважену національну політику щодо посилення співпраці у сфері кібербезпеки. Враховуючи загрозливі тенденції глобальної цифровізації, зростання транснаціональної кіберзлочинності та динамічне поширення кіберзагроз у глобальному масштабі, для України є актуальним уточнення напрямків подальшої міжнародної співпраці у зміцненні можливостей України у сфері кібербезпеки.

Статтею 14 Закону України «Про основи забезпечення кібербезпеки України»[86] визначено, що міжнародне співробітництво у сфері кібербезпеки здійснюється нашою державою відповідно до міжнародних договорів, укладених з іноземними державами, їх правоохоронними органами. та спецслужбами, а також співпрацею з міжнародними організаціями з питань транснаціональної кіберзлочинності.

Відповідно до чинного в Україні законодавства про зовнішній зв’язок, суб’єкти кібербезпеки в межах своєї компетенції можуть безпосередньо здійснювати міжнародне співробітництво у сфері кібербезпеки на дво- або багатосторонній основі. Про доцільність підвищення рівня кібербезпеки, в тому числі шляхом міжнародного співробітництва, зазначено в Указі Президента України від 20 грудня 2019 року, яким введено в дію рішення Ради національної безпеки і оборони України від 7 грудня 2019 року «Про зміцнення національних можливостей у сфері кібербезпеки «Надзвичайні заходи для будівництва» [87].

Виходячи з теоретичної бази чинного законодавства, Україна співпрацює у сфері кібербезпеки з іноземними державами, своїми збройними силами, правоохоронними органами та спецпідрозділами, переважно з державами-членами НАТО та ЄС, а також з міжнародними організаціями, відповідно до укладених нею міжнародних договорів. Цей формат охоплює широкий спектр нормативних, методичних, практичних, наукових та освітніх питань, включаючи проведення тематичних міжнародних семінарів та конференцій, надання структурованої та практичної допомоги іноземним партнерам, а також організацію робочих контактів з провідними експертами у сфері кібербезпеки, з позитивними Результати дослідження та впровадження найкращих практик кіберзахисту у визнаних областях [88]

Тому міжнародне співробітництво є критичню необхідністю для усунення правового вакууму, який існує між динамічним розвитком інформаційних технологій і законодавчою відповіддю на сучасні кіберзагрози. Метою міжнародного співробітництва є: зміцнення взаємної довіри у сфері кібербезпеки; розробка спільного підходу до протидії кіберзагрозам; посилення виявлення та попередження кіберзлочинності та запобігання використанню кіберпростору в протиправних цілях; у контексті співпраці між відомствами та спецпідрозділи та міжнародними організаціями у сфері кібербезпеки, виконувати свої зобов’язання в рамках укладених міжнародних договорів, оптимізувати надання міжнародної технічної допомоги [89].

У сучасних умовах ситуація навколо майбутнього глобального кіберпростору знаходиться на перетині двох егалітарних тенденцій. З одного боку, офіційні зусилля міжнародної спільноти спрямовані на демілітаризацію кіберпростору та недопущення його перетворення на нове поле збройних конфліктів, а з іншого боку, фактично триває процес біполярного протистояння. Незважаючи на те, що міжнародні організації, такі як ООН, намагаються вплинути на процес, ці наміри досить часткові. Незважаючи на

численні рішення та резолюції, ООН ще не запроваджено ефективне міжнародне право механізму оптимізації питань безпеки мережі.

Значна кількість документів ООН з цього приводу є суперечливими, а деякі країни-члени не вважають його фундаментальним документом[90]. Хоча останнім часом Організація Об'єднаних Націй демонструє все більшу активність на регулятивній арені глобальних питань кібербезпеки. Наприклад, у червні 2015 року, згідно з результатами засідання Міжнародної групи урядових експертів ООН з питань інформаційної безпеки, було визнано, що міжнародне право застосовується до використання інформаційно-комунікаційних технологій, але може бути доповнено, якщо необхідно, у тому числі через прийняття нових норм.

Модернізація політики інформаційної безпеки на рівні ООН залежить від нових елементів відповідальної поведінки держав, приватного сектору, наукових кіл та громадянського суспільства в кіберпросторі, що може сприяти ефективності міжнародного співробітництва [91].

З 2019 року відбулася значна зміна парадигми, в якій тема злочинів у сфері інформаційних технологій обговорюється та схвалюється Організацією Об'єднаних Націй, що пов'язано зі швидким поширенням глобальних гібридних загроз у міжнародному масштабі цієї галузі. Останнім часом робота на рівні експертів ООН була активізована для розробки міжнародного інструменту розробки єдиного підходу для адекватного вирішення сучасних викликів, оскільки світ страждає від нерівномірного розподілу та нерівного управління життєво важливими ресурсами системи Інтернету, що створює проблеми та загрози безпеці, пов'язані з безперебійною роботою архітектури. У цьому контексті всі країни повинні брати участь в управлінні та розподілі міжнародних Інтернет-ресурсів на рівних принципах і рівних засадах. Менеджери критично важливих ресурсів не повинні бути під контролем жодного уряду. Однак головним питанням, яке стосується ООН, є застосування чинного міжнародного права в кіберпросторі [92].

28 грудня 2019 року Генеральна Асамблея ООН схвалила резолюцію про боротьбу з кіберзлочинністю. Зокрема, «проти» резолюції виступають США, Канада, країни Європи, а особливо Україна. Авторами документу є 47 країн, зокрема Російська Федерація, Білорусь, Казахстан, Азербайджан, Таджикистан, Вірменія, Китай, Індія, Сирія, Єгипет, КНДР, Іран і Венесуела. Документ передбачає створення міжнародного комітету з метою розробки міжнародної конвенції про боротьбу зі злочинами у сфері інформаційних технологій, яка б мала набути чинності в серпні 2020 року. Сполучені Штати та Європейський Союз вважають, що запропонована ініціатива може призвести до встановлення інтернет-цензури. а обмеження свободи слова в глобальних мережах становить реальну загрозу.

У представництві США в ООН заявили, що прийнята резолюція не є випадковістю, яка може підірвати міжнародну співпрацю проти кіберзлочинності. Навіть міжнародна правозахисна організація Human Rights Watch підкреслила, що резолюція ухвалена державами, передусім Російською Федерацією, яка використовує репресивні методи боротьби з інакомисленням. Україну також обурила законодавча ініціатива ООН, адже ця міжнародна структура, певною мірою співпрацюючи з державою-агресором, фактично запропонувала проект постанови з метою розширення свого впливу в кіберпросторі, отримання легального доступу до «блокування інформації в Інтернеті», значно обмежуючи цифрові права громадян. Пропозиція держави-агресора щодо такого закону в ООН базується на федеральному законі Російської Федерації «Суверенні руни», який набув чинності 1 листопада 2019 року, основною концепцією якого є створення інфраструктури, яка дозволить Кремлю ізолювати Росією частину Інтернету і фільтрувати внутрішній і зовнішній інтернет-трафік.

Очікується, що майбутня робота ООН, особливо Групи урядових експертів ООН з інформаційної безпеки, буде зосереджена на чотирьох ключових сферах: 1) правила, норми та принципи поведінки держав в інформаційному просторі; 2) заходи, спрямовані на зміцнення довіри до

нього 3) нарощування цифрового потенціалу; 4) інституціоналізувати переговорний механізм ООН з питань міжнародної інформаційної безпеки [93].

Враховуючи сучасні виклики та загрози, Україні вкрай необхідно забезпечити участm в Міжнародній платформі дій Генеральної Асамблеї ООН із заохочення відповідальної поведінки держав у кіберпросторі та Групі урядових експертів ООН з інформації (UNGGE).

Найвпливовішою та найавторитетнішою міжнародною структурою є НАТО, який постійно вдосконалює власну безпекову політику, яка трактує кіберпростір як арену протистояння та середовище для інформаційної війни, визначаючи кібербезпеку головним пріоритетом своєї діяльності. Союзники підтвердили оборонну місію НАТО та визнали, що кіберпростір є оперативним середовищем, у якому НАТО має ефективно захищатися, а також в інших фізичних середовищах, таких як конфронтація.

Місія командування реагування на кіберзагрози НАТО полягає в тому, щоб допомагати союзникам реагувати на кібератаки. Крім того, для захисту країн-членів НАТО національні підрозділи кібербезпеки можуть брати участь у спецопераціях. Зокрема, у 2019 році були схвалені рекомендації НАТО, які містили кілька інструментів: проактивне посилення адекватного реагування на кібератаки, активізація співпраці з бізнес-партнерами та бізнес-середовищем у сфері розвитку кіберіндустрії, у консалтингу та безпеці, створення можливостей для союзників використовувати кіберпростір на нормативній основі [94].

Для України одним із пріоритетів міжнародного співробітництва у сфері кібербезпеки залишається стратегічне партнерство з Північноатлантичним альянсом. Водночас основними завданнями співпраці НАТО та країн-партнерів у сфері кіберзахисту залишаються: підтримка нормальної життєдіяльності критичної інформаційно-комунікаційної інфраструктури; розробка ефективних заходів протидії кібератакам; допомога державам-членам у відновленні відповідної інфраструктури,

викликаної шляхом зовнішніх кібератак; нормальне функціонування системи функціонування яка оперативно реагує на будь-яку загрозу в інформаційній сфері держав-членів [95].

Основні принципи співпраці між НАТО та країнами-партнерами у сфері кіберзахисту передбачають: Альянс може надавати експертну допомогу країнам-партнерам, коли це необхідно, і може надавати можливість захисту від кібератак; країни-партнери можуть подавати заявки на співпрацю у сфері кіберзахисту, а також у разі національного отримання підтримки НАТО у разі значної кібератаки; співпраця між НАТО та країнами-партнерами має бути взаємовигідною, оскільки альянс може надавати інформацію та підтримку партнеру, але, у свою чергу, отримувати необхідну інформацію та підтримку з боку партнера, зокрема це стосується досвіду у сфері спілкування.

НАТО та її партнери повинні уникати дублювання заходів, вжитих в рамках інших міжнародних організацій, які займаються захистом інформаційних систем від кібератак; чи існує угода про безпеку між НАТО та країнами-партнерами, яка визначатиме обсяги допомоги та обміну інформацією. Світовий досвід переконливо доводить, що національну безпеку неможливо уявити без умов: вдосконалення національної системи забезпечення кібербезпеки відповідно до критеріїв вступу України до НАТО, підтримки міжнародних ініціатив у сфері кібербезпеки, зміцнення співпраці з Україною [96].

У липні 2019 року Польща та НАТО підписали першу угоду про співпрацю у сфері кібербезпеки. Комплексна взаємодія передбачає використання можливостей НАТО, спрямованих на нейтралізацію загроз у кіберпросторі, створення цілодобової точки швидкого реагування на кіберінциденти. Угода стала юридичною основою для можливого використання альянсом груп швидкого реагування в міру поширення загроз у кіберпросторі. Завдяки угоді Польща братиме участь у розробці системи раннього попередження про загрози в кіберпросторі, а також може

покладатися на поради експертів НАТО та плідну співпрацю з оборонною промисловістю. На цьому тлі очевидна міжнародна співпраця між Україною та НАТО з питань кібербезпеки.

Одним із основоположних аспектів безпекової політики України залишається конструктивне партнерство з НАТО, яке базується на критеріях реагування на сучасні виклики та загрози. У рамках розвитку міжнародного співробітництва у сфері кібербезпеки в Україні особливе партнерство з НАТО є невід'ємною частиною євроінтеграційного процесу, оскільки воно доповнює внутрішній процес трансформації необхідними оборонними та безпековими реформами сектору. Практика, що склалася в цій формі, передбачає щорічне затвердження національного плану співробітництва Україна-НАТО на державному рівні [97].

Указом Президента України затверджено Порядок розроблення, моніторингу та оцінки результатів виконання річного національного плану під егідою Комітету Україна-НАТО. Аналіз цього програмного документу доводить, що співпраця з НАТО не обмежується реформами у сфері безпеки. Річний національний план під головуванням Комітету Україна-НАТО є ключовим інструментом досягнення Україною необхідних критеріїв для членства в НАТО. Це системний документ, що містить опис реформи, визначення стратегічної мети, змісту, завдань і заходів реформування, зокрема політичні та економічні, оборонні та військові питання, проблеми ресурсного забезпечення, безпекові та правові питання.

Зокрема, уряду доручено щорічно затверджувати перелік заходів щодо виконання річного державного плану та показників ефективності його виконання, координувати діяльність центрального органу виконавчої влади та інших державних органів щодо моніторингу та оцінки результатів. Виконувати річний національний план, регулярно інформувати громадськість про хід і результати виконання річного національного плану.

У сьогоднішніх умовах країни-члени НАТО надаватимуть підтримку Україні через Трастовий фонд кібербезпеки для розвитку її обороноздатності

у сфері кібербезпеки, включаючи надання обладнання, програмного забезпечення, технічної допомоги, консалтингових послуг та навчання[98]. Серед інших донорів довірчого фонду є такі країни: Албанія, Італія, Туреччина та Сполучені Штати. Враховуючи можливості та потенціал Трастового фонду НАТО, до основних заходів, реалізація яких дозволить зміцнити кібербезпеку нашої держави, належать: проведення експертних консультацій з питань кібербезпеки, започаткування діяльності фонду щодо формування базової ідеї національного система кібербезпеки.

Керівництво НАТО визнає Румунію членом Європейського Союзу та є головною країною для трастового фонду, координаторами якого є румунські сили спеціального призначення та Державна румунська компанія «RASIROM RA», що спеціалізується на інтеграції та розробці систем кібербезпеки. Перспективний розвиток оборонно-технологічного потенціалу України у сфері кібербезпеки досягається шляхом: впровадження передових технологічних рішень у критичній інфраструктурі для забезпечення належного рівня кібербезпеки, надання експертизи в комп'ютерних технологіях зі стаціонарними та мобільними компонентами, створення центральних та кіберлабораторій; навчання персоналу, включаючи навчання групи реагування на інциденти кібербезпеки (CERT) щодо експлуатації, обслуговування та управління створеними інформаційними системами. Виходячи з цього, найактуальнішим і найважливішим завданням Трастового фонду кібербезпеки є допомога Україні у розвитку технічних можливостей протидії сучасним кіберзагрозам [99].

У липні 2017 року Служба безпеки України провела урочисту церемонію завершення першої фази проекту Трастового фонду НАТО для допомоги Україні у зміцненні її спроможностей у сфері кібербезпеки. Загальна сума, яка буде відрахована з трастового фонду на першому етапі, становить 1 мільйон євро. Окрім надання обладнання та програмного забезпечення, програма також покриває витрати на навчання працівників. Ще у 2018 році в Києві було створено перший Центр

кібербезпеки, створений в рамках Угоди про реалізацію трастового фонду Україна-НАТО. За результатами роботи у 2018 році Трастовий фонд кібербезпеки повністю реалізував перший етап перед переходом до другого етапу, який зараз триває. У цьому контексті конструктивна співпраця з НАТО залишається актуальним напрямком міжнародного співробітництва у сфері кібербезпеки, зокрема: консультації та переговори з питань кібербезпеки, продовження вдосконалення нормативно-правової бази з питань кібербезпеки, забезпечення та сприяння розвитку під егідою Альянсу. Як наслідок, державою проведено заходи щодо прискорення впровадження стандартів НАТО у сфері приєднання до колективної системи кіберзахисту [100].

Загалом можна сказати, що Україна веде конструктивний діалог з НАТО у сфері кібербезпеки. У цьому контексті Україна має розвивати міжнародне співробітництво у сфері кібербезпеки, підтримувати міжнародні ініціативи у цій сфері, у межах напрямів, які становлять національний інтерес України, а також поглиблювати діалог між Україною та Організацією з безпеки та співробітництва в Європі щодо зміцнення довіри у використанні засобів кібербезпеки. У майбутньому динамічний розвиток співпраці з НАТО у сфері кібербезпеки буде плідним, якщо українські політичні лідери насамперед підтримають темпи реформ у військовій та оборонній сферах та підвищать рівень міжвідомчої взаємодії та координації.

Україна має продовжити участь у міжнародному діалозі щодо відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН та норм, правил і принципів відповідальної поведінки держав. Це вимагатиме більшої координації та консолідації зацікавлених сторін на міжнародних форумах, де Україна буде не лише учасником, а й ініціатором та організатором. Враховуючи вищезазначене, Україна повинна займати більш активну позицію на міжнародній арені з питань кібербезпеки. Країна має розвивати міжнародне співробітництво у сфері кібербезпеки, перш за все, для забезпечення

суверенної незалежності країни, відновлення територіальної цілісності України та підтримки ініціатив учасників системи колективної безпеки НАТО[101]. З цією метою слід прискорити такі заходи: енергійно розвивати міжнародне співробітництво у сфері кібербезпеки шляхом підтримки міжнародних ініціатив в національних інтересах України, поглибити діалог між Україною, НАТО та ЄС, особливо щодо посилення використання кіберпростору у напрямку довіри, спільного розуміння кіберзагроз та вдосконалення таких рівноправних механізмів співпраці, визначення та затвердження переліку пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки в Україні. Іншими словами, продовження партнерства з НАТО в кіберсфері залишається актуальним напрямком для України. При цьому основними зовнішньополітичними напрямками України у сфері кібербезпеки є: поглиблення євроінтеграційного процесу шляхом уніфікації методів, способів і засобів забезпечення кібербезпеки з усталеними практиками НАТО, вжиття інших погоджених із іноземними партнерами заходів, спрямованих на посилення кіберстійкості в Україні; розвиток можливостей національної системи кібербезпеки для захисту національних інтересів у кіберпросторі.

ВИСНОВКИ

Дослідивши визначену метою роботи проблематику, ми дійшли наступних висновків.

Гіперактивність Росії в кіберпросторі є головним викликом і загрозою, з якою стикається Україна у сфері кібербезпеки. Російська Федерація використовує кіберпростір як простір нових можливостей для проведення не лише розвідувально-підривної діяльності проти України, а й спеціальних операцій з прихованого проникнення в кібермережі органів державної влади та управління, дистанційного контролю об’єктів критичної інфраструктури для отримання інформації у військово - політичній, фінансово-економічній та енергетичній сферах.

Слід зазначити, що на сьогодні ні в доктрині, ні на практиці чітко не визначено поняття комп’ютерної злочинності, дискутуються різні погляди на її класифікацію. Формування цих понять є складним через неможливість виокремлення єдиного об’єкта злочинного посягання.

Аналіз стратегій міжнародного співробітництва у сфері протидії кіберзлочинності на сучасному етапі показує, що концепції, теорії та методи застосування міжнародних організацій для здійснення міжнародного співробітництва у цій сфері мають як спільні, так і відмінні риси, які зумовлені різними поглядами на пріоритети в цій галузі. Інформаційна безпека країн-учасниць цих інституцій, у свою чергу, пов'язана з різними рівнями їх інформаційного розвитку.

Більшість країн надають великого значення таким питанням, як інформаційна безпека, управління Інтернетом, формування загальноприйнятих міжнародних правил і норм, визнаючи необхідність співпраці та взаємних консультацій відповідно до Статуту ООН, міжнародного законодавства та основних принципів міжнародних відносин.

Прагнення створити стійке, стабільне та безпечне суспільство об’єднує міжнародну спільноту та сприяє партнерству, співпраці та взаєморозумінню. Особливістю процесу забезпечення міжнародної інформаційної безпеки стала багатостороння участь. ООН бере активну участь у процесі сприяння глобальному розвитку та розбудові безпечного світового суспільства. Гострою та актуальною в сучасному світі є тема міжнародного співробітництва у забезпеченні міжнародної безпеки загалом, та інформаційної зокрема. В рамках Організації Об’єднаних Націй та через механізм Організації Об’єднаних Націй міжнародне співтовариство продемонструвало прагнення до широкомасштабної співпраці, спільних зусиль, взаємодії, спільної участі, відкритості та прозорості, відповідальності та інновацій у вирішенні спільних проблем у безпечній світ.

Аналіз європейського досвіду боротьби зі злочинністю в інформаційній сфері підтверджує, що цьому питанню приділяється значна увага зі сторони Європейського Союзу. Питання боротьби з дезінформацією опинилося в центрі уваги науковців і практиків лише останніми роками.

Дотримуючись думок вітчизняних експертів, вважаємо, що при формуванні регламенту діяльності вітчизняних правоохоронних органів завжди слід враховувати регламент взаємодії з Інтерполом та реалізовувати його через такі механізми:

- норми та закони, що забезпечують гармонізацію національного законодавства з процесуальними нормами Інтерполу у сфері запобігання та протидії злочинності та зміцнення правового статусу Служби національної безпеки Інтерполу в Україні;

- економія, можливість співфінансування спільних операцій Інтерполу, матеріальне стимулювання представництва України в Генеральній Асамблеї та Національному центральному бюро, реформування діяльності вітчизняних правоохоронних органів відповідно до завдань Інтерполу;

- адміністрація та організація, що передбачають наявність організаційної приналежності, підзвітності, управління організаціями по запобіганню та боротьбі зі злочинами у сфері інформаційних технологій;

- контроль, який передбачає вжиття заходів контролю за діяльністю правоохоронних органів, визначення ключових моментів діяльності та розробку рекомендацій щодо вдосконалення окремих механізмів та державної політики у сфері протидії злочинам, вчиненим за допомогою інформаційних технологій.

Наразі статус міжнародного співробітництва у сфері протидії злочинам у сфері інформаційних технологій є незрозумілим. З одного боку, велика кількість країн, які беруть участь у такій співпраці, дозволяє нам охоплювати та контролювати понад 80% взаємовідносин у сфері інформаційно-комп'ютерних технологій. З іншого боку, ефективність засобів міжнародно-правової боротьби залишається низькою.

По-перше, це пояснюється об'єктивними причинами, зокрема невідповідністю між інтенсивністю появи засобів кіберзлочинності та своєчасністю правового реагування міжнародної спільноти.

По-друге, існує проблема узгодженості дій країн-учасниць і швидкості спільних дій, ключ до вирішення якої полягає у взаємній відкритості національного законодавства. Крім того, взаємодія країн у боротьбі з кіберзлочинністю вимагає від правоохоронних органів проникнення один одного на арену зв'язків з громадськістю, де інформація часто є комерційною таємницею або містить персональні дані з обмеженим доступом. Інакше кажучи, вважається, що пошук шляхів підвищення ефективності протидії кіберзлочинності полягає у вирішенні протиріч у сфері правового регулювання інформаційного простору та встановленні єдиних правил його використання як у приватному, так і в бізнес-користуванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біленчук П., Малій М. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи?//Юридичний Вісник України, 2019.-No39.-с.14-15.

2. Revised Assessment Report (2018) on International cooperation on cybercrime in the Eastern Partnership region [Електронний ресурс] // Cybercrime Programme Office of the Council of Europe under the Cybercrime@EAP 2018 Project. – 2018. – Режим доступу до ресурсу: https://rm.coe.int/cybercrime-eap-international-cooperation-report-rev-2018/16807f584d.

3. Inter-American Cooperation Portal on Cyber-Crime. [Електронний ресурс] // Department of Legal Cooperation. OAS – Режим доступу до ресурсу: http://www.oas.org/juridico/english/cyber.htm.

4. Security and Prosperity Steering Group [Електронний ресурс] // Asia Pacific Economic Cooperation – Режим доступу до ресурсу: https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group.

5. Бойченко О. В. Угрозы информационных ресурсов государственного самоуправления / О. В. Бойчен- ко // Материалы Международной научно-практической конференции «Проблемы и особенности влияния международной информации на экономические и общественно-политические процессы». – Симферополь : ИСВА МСУ, 2007. – С. 39–41.

6. Пилипчук В. Г., Брижко В. М. Реформування і розвиток системи захисту персональних даних в Україні // Інформація і право. 2017. № 3. С. 5–21.

7. Пилипчук В. Г., Брижко В. М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України // Вісник Національної академії правових наук України. 2017. № 3. С. 36–50.

8. В. Бутузов Системно-структурний аналіз як метод дослідження протидії комп'ютерній злочинності / В. Бутузов // Правова інформатика. - 2011. - № 1. - С. 67-71. – Режим доступу: http://nbuv.gov.ua/UJRN/Pinform_2011_1_13.

9. Войцехівський А. Міжнародне співробітництво в боротьбі з кіберзлочинністю / А. В. Войціховський // Право і Безпека. - 2011. - № 4. - С. 107-112. - Режим доступу: http://nbuv.gov.ua/UJRN/Pib_2011_4_26

10. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності // Право і безпека. – 2015. – No 2(57). – С. 107-113

11. Палієнко М. Актуальні питання захисту персональних даних та збереження приватних архівів на 28-му Міжнародному архівному форумі у м. Трієст (Італія) // Архіви України. 2018. № 5–6. С. 234–243.

12. Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю / Сироїд Те- тяна Леонідівна // 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.

13. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. – Київ : КНТ, 2007. – 160 с.

14. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

15. Васильєв А. А. Особливості кваліфікації кіберзлочинів проти власності / Васильєв Андрій Анатолійович, Пашнєв Дмитро Валентинович // Проблеми правознавства та правоохоронної діяльності. - 2016. - № 4 (58). - С. 136-143.

16. Голубєв В.О. Інформаційна безпека : проблеми боротьби з кіберзлочинами / В.О. Голубєв. – Запоріжжя, 2019. – С. 79-84.

17. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. ... канд. юрид. наук : 12.00.01 / Максименко Юлія Євгеніївна. – Київ, 2007. – 20 с.

18. Мещеряков В.А. Сліди злочинів у сфері високих технологій. Бібліотека криміна-листу. 2013. No 5 (10). С. 265-269.

19. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva [Електронний ресурс] / Stein Schjolberg. – 2018. – Режим доступу до ресурсу: http://cybercrimelaw.net/documents/cybercrime_history.pdf

20. Звіт щодо України про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них від 3 .11.2016./ Project Cybercrime@ESP III . [Електронний ресурс] . – Режим доступу: https://rm.coe.int/16806f3743

21. Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime [Електронний ресурс] // Cybercrime Convention Committee (T-CY). – 2017. – Режим доступу до ресурсу: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

22. Резолюция, принятая Генеральной Ассамблеей 65/230. Борьба с преступным использованием информационных технологий [Електронний ресурс] // ГА ООН. – 2010. – Режим доступу до ресурсу: https://documents-dds- ny.un.org/doc/UNDOC/GEN/N10/526/36/PDF/N1052636.pdf?OpenElement

23. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / Тарасюк А. В. : монографія / А. В. Тарасюк. – Київ; Одеса : Фенікс, 2020. – 404 с.

24. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.

25. Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and particularities (Захист права власності в суді) // Asia life science, Supplement 21(2), December2019. Iss. 2. P. 863-879. Філіпини. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85077221643&origin=resultslist

26. Юхно О. О., Загуменний О. О. Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних слідчих (розшукових) дій : навч. посіб. / Видання друге, доп. і перероб. (Серія «Бібліотека слідчого і детектива: проблеми кримінального процесу») Харків : Колегіум, 2020. 116 с.

27. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Науковий журнал Право і Безпека. 2021. No4. http://archive.nbuv.gov.ua/portal/soc_gum/pib/ 2011_4/PB–4/PB–4_26.pdf

28. І. О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційнопошукових систем для забезпечення проведення негласних слідчих (розшукових) дій. Право і Безпека : науковий жур- нал. No 4 (46) за 2012 рік. Харківський національний університет внутрішніх справ : видавництво ХНУВС. 2019. 360 с.

29. Гуславський В. С., Задорожній Ю. А., Розовський В. Г. Інформаційно-аналітичне забезпечення розкриття та розслідування злочину: монографія Луганськ. ТОВ "Елтон2", 2018. 133 с.

30. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. No 1(28)/2019. С. 108-117.

31. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / Тарасюк А. В. : монографія / А. В. Тарасюк. – Київ; Одеса : Фенікс, 2020. – 404 с.

32. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. – Режим доступу : //www.zakon2.rada.gov.ua/laws/show/994_575

33. Алавердов О.С. Міжнародне співробітництво у сфері боротьби з Інтернет-злочинністю / О.С. Алавердов // Суспільство право. - 2020. - No 3.

34. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству [Електронний ресурс] / М. І. Саєнко, Є. А. Савела, Ю. Ю. Тополянський // Науковий вісник Ужгородського національного університету. Серія : Право. - 2021. - Вип. 64. - С. 386-391.

35. Біленчук Д.П. Кібрешахраї – хто вони? // Міліція України. – 1999. – No 7-8. – С. 32-34.

36. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. – Режим доступу : //www.zakon2.rada.gov.ua/laws/show/994_575

37. Леонов Б. Д. Методичне забезпечення заходів з класифікації ідентифікації та фіксації кіберзлочинів [Електронний ресурс] / Б. Д. Леонов, В. С. Серьогін // Інформація і право. - 2021. - No 1. - С. 99-105

38. Гладка Н. М. Боротьба з кіберзлочинністю: напрями вдосконалення кримінального законодавства України [Електронний ресурс] / Н. М. Гладка // Науковий вісник Ужгородського національного університету. Серія : Право. - 2020. - Вип. 60. - С. 139-142.

39. Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація / О. В. Таволжанський // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право. - 2017. - No 4. - С. 158-164

40. Карчевський М.В. Правове регулювання соціалізації штучного інтелекту. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Науково-теоретичний журнал. 2017. С. 99-08.

41. Резолюция Генеральной Ассамблеи ООН A/RES/55/63 «Борьба с преступным использованием информационных технологий» [Електронний ресурс]. – Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/19/PDF/N0056319.pdf

42. Резолюция Генеральной Ассамблеи ООН A/RES/56/121 «Борьба с преступным использованием информационных технологий» [Електронний

ресурс]. – Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/482/06/PDF/N0148206.pdf

43. Резолюция Генеральной Ассамблеи ООН A/RES/57/239 «Элементы для создания глобальной культуры кибербезопасности» [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml.

44. Резолюция Генеральной Ассамблеей A/RES/58/140 «Укрепление Программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в особенности ее потенциала в сфере технического сотрудничества» [Електронний ресурс]. – Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/503/00/PDF/N0350300.pdf

45. Резолюция Генеральной Ассамблеей A/RES/58/199 «Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур» [Електронний ресурс]. – Режим доступу: https://documents-ddsny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf

46. Зміцнення Програми Організації Об'єднаних Націй у галузі запобігання злочинності та кримінального правосуддя, особливо її потенціалу у сфері технічного співробітництва A/RES/63/195 [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/482/51/PDF/N0848251.pdf

47. Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства. Матеріали офіц. сайту [Електронний ресурс]. – Режим доступу: http://www.un.org/ua/events/pastevents/wsis.shtml.

48. Декларація принципів Побудова інформаційного суспільства – глобальне завдання новому тисячолітті. Документ WSIS-03/GENEVA/DOC/4-R [Електронний ресурс]. – Режим доступу: http://www.un.org/ua/events/pastevents/pdf/dec_wsis.pdf.

49. План дій. Док. WSIS-03/GENEVA/DOC/5-R [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/events/pastevents/pdf/plan_wsis.pdf.

50. Туніська програма для інформаційного суспільства. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf.

51. Доповідь Генерального секретаря A/70/63-E/2015/10 «Прогрес, досягнутий у здійсненні рішень та подальшої діяльності за підсумками Всесвітньої зустрічі на найвищому рівні з питань інформаційного суспільства на регіональному та міжнародному рівнях» [Електронний ресурс]. – Режим доступу: http://unctad.org/en/PublicationsLibrary/a70d63_ua.pdf.

52. Резолюція Генеральною Асамблеєю A/RES/65/230 «Дванадцятий Конгрес Організації Об'єднаних Націй щодо попередження злочинності та кримінального правосуддя» [Електронний ресурс]. – Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/526/36/PDF/N1052636.pdf

53. Резолюція Генеральної Асамблеї A/RES/69/204 «Використання інформаційно-комунікаційних технологій для розвитку» [Електронний ресурс]. – Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/711/45/PDF/N1471145.pdf

54. Резолюція Генеральної Асамблеї A/RES/70/237 «Досягнення в сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» [Електронний ресурс]. – Режим доступу: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/60/PDF/N1545760.pdf {jcomments on}

55. Bonacquisti G. The solidarity clause: one of the most unacknowledged innovations of the Lisbon Treaty. The European Par- liament debates its implementation but also its ambiguities. URL: https://europe-liberte-securite-justice.org/2015/07/27/the-solidarity- clause-one-of-the-most-unacknowledged-innovations-of-the-lisbon-treaty-the-european-parliament-debates-its-implementation-but- also-its-ambiguities/ (accessed 12.02.2018).

56. Fletcher M. EU criminal law and justice / M. Fletcher, R. Lööf, B. Gilmore. Cheltenham: E. Elgar, 2008. 235 p.

57. Macdonald S. Cyberterrorism and enemy criminal law // Cyber War: Law and Ethics for Virtual Conflicts / ed. by Ohlin J. D and oth. URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2667611_code359596.pdf?abstractid=2667611&mirid=1&type=2.

58. Research Handbook on Cross-border Enforcement of Intellectual Property / ed. by P. Torremans. Cheltenham: Edward Elgar Publishing, 2014. 889 p.

59. Speer D. L. Redefining borders: the challenges of cybercrime // Crime, Law Social Change. 2000. Vol. 34. No 3. P. 259–273.

60. Walden I. Harmonising computer crime laws in Europe // Europ. J. of Crime, Criminal Law a. Criminal Justice. 2004. Vol. 12. No 4. P. 321–336.

61. Wessel R. A. Towards EU cybersecurity law: Regulating a new policy field // Research Handbook on International Law and Cyberspace / ed. by N. Tsagourias, R. Buchan. Cheltenham: E. Elgar. P. 403–425.

62. Борисов Д.А. 2018. Екстремізм і контртерористичний порядок денний ООН у XXI столітті. – Світова політика. No 1. С. 48-57.

63. Бочарніков І.В. 2013. Інформаційна протидія тероризму в сучасних умовах. - Електронний науковий журнал проблем безпеки. No 3 (21). З. 2-3. Доступ: https://elibrary.ru/item.asp?id=21292041

64. Туронок С.Г. Інформаційний тероризм: вироблення стратегії протидії. – Суспільні науки та сучасність. No 4. - 2011. - С. 131-140

65. 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. URL: https://www.researchgate.net/publication/328433593_The_Present_and_Future_of_Cybercrime_Cyberterror-ism_and_Cybersecurity

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

https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/

67. Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки. Доповідь Генерального секретаря ООН. No A/71/172, 19 липня 2019 р. [Електронний ресурс]. – Режим доступу: http://undocs.org/ua/A/71/172

68. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. Ю. Шостко та ін.; за ред. Б. М. Головкіна. – Харків : Право, 2020

69. Войтюк Р. В. Порівняльний аналіз детектива Національного антикорупційного бюро України та комісара Незалежної антикорупційної комісії Гонконгу // Науковий вісник Національної академії внутрішніх справ. – 2017. – № 1. – С. 346-358.

70. Статут Міжнародної організації кримінальної поліції Інтерполу (набрав законної сили 13 червня 1956 року, із змінами, внесеними згідно з станом на 1 січня 1986 р. // [Електронний ресурс] / Верховна Рада України; офіційний веб-сайт. – Режим доступу до сайту: http://zakon.rada.gov.ua/laws/show/995_142.

71. Про вступ України до Інтерполу: Постанова Кабінету Міністрів України від 30 вересня 1992 року № 555 // [Електронний ресурс] / Верховна Рада України; офіційний веб-сайт. – Режим доступу до сайту: http://zakon.rada.gov.ua/laws/show/555-92-%D0%BF.

72. Про Національне центральне бюро Інтерполу: Постанова Кабінету Міністрів України від 25 березня 1993 року № 220 із змінами, внесеними згідно з Постановами КМ № 532 від 13.06.2012 № 968 від 13.12.2017 // [Електронний ресурс] / Верховна Рада України; офіційний веб-сайт. – Режим доступу до сайту: http://zakon.rada.gov.ua/laws/show/220-93-п.

73. Леженіна О.І. Організаційно-правові засади участі органів внутрішніх справ України у міжнародній правоохоронній діяльності : автореф. дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове

право; інфор- маційне право» / О.І. Леженіна ; Національний ун-т внутрішніх справ. – Х., 2004. – 20 с.

74. Абу Давас Басе Мохамед. Становлення та розвиток міждержавних організацій по боротьбі з міжнародною злочинністю (кримінально-правове дослідження на матеріалах України та Молдови): автореф. дис. ... д-ра права: спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / Абу Давас Басем Мохамед; Міжнародний незалежний університет Молдови. – Кишинів. 2001. - 22 с.

75. Філяніна Л.А., Лінській В.І. Порядок здійснення правоохоронними органами міжнародного розшуку, затримання та видачі злочинців (екстрадиції): Науково-методичні рекомендації. – Д.: Дніпроп. держ. ун-т внутр. справ, 2006. – 64 с.

76. Карпов О.Н. Використання можливостей міжнародних поліцейських організацій у розшуку злочинців : автореф. дис. ... канд. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / О.Н. Карпов ; Національна академія внутрішніх справ. – К., 2011. – 20 с.

77. Чорноус Ю.М. Криміналістичне забезпечення досудового слідства у справах про злочини міжнародного характеру : автореф. дис. ... док. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-роз- шукова діяльність» / Ю.М. Чорноус ; Національна академія внутрішніх справ. – К., 2013. – 31 с.

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

79. Конвенції про кіберзлочинність від 23 листопада 2001 року [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/ laws/show/994_575

80. Голубєв В.О. Проблеми боротьби зі зло-чинами у сфері використання комп’ютерних технологій [Текст]: навч. посіб./ В.О. Голу- бєв, В.Д.

Гавловський, В.С. Цимбалюк та ін.; за ред. д.ю.н., професора Р.Н. Калюжного.— Запоріжжя: ГУ «ЗІДМУ», 2002. — 292 с.

81. Скулиш Є.Д. Посилення відповідальності в контексті підвищення ефективності боротьби із кіберзло- чинністю. *Правова інформатика*. 2020. No 4 (40). С. 90–97.

82. Грицун О.О. Регулювання питань міжнародної інформаційної безпеки в межах міжнародних організацій/ О.О. Грицун // Ві- сник Запорізького національного університе- тету.— No 4 (I).— 2014.— 172-180.

83. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року [Електронний ре- сурс]. – Режим доступу: http://base. spinform. ru/show_doc.fwx?rgn=28340.

84. Хлапонін Ю.І., Кондакова С.В., Шабала Є.Є., Юрчук Л.П., Демяечук П.С. Аналіз стану кібербезпеки в провідних країнах світу. Кібербезпека: освіта, наука, техніка. 2019. Вип. 4. Т. 4. С. 6–13.

85. Марков В.В. До питання щодо зарубіжного дос-віду протидії кіберзлочинності. Право і безпека. 2015. No 2 (57). С. 107–113.

86. Захист державних інформаційних ресурсів України 30.12.2020 – 05.01.2021. URL : https://cip.gov. ua/ua/news/operativna-informaciya-derzhspeczv-yazku- shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-30-grudnya-2020-po-05-sichnya-2021-roku

87. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05.10.17 р.№ 163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

88. Про рішення Ради національної безпеки і оборони України від 7 грудня 2019 року "Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки". Указ Президента України від 20.12.19 р. № 923/2019 URL: https://zakon.rada.gov.ua/laws/show/923/2019#Text

89. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. Вісник Національної академії

державного управління при Президентові України. Серія: “Державне управління". 2015. № 4. С. 50-56. URL: http://nbuv. gov.ua/UJRN/Vnadu 2015 4 10

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

91. Демедюк С.В., Демедюк Т.С. Міжнародний досвід протидії кіберзлочинності, Вісник Харківського національного університету внутрішніх справ. 2014. № 4. С. 65-75. URL: http://nbuv.gov.ua/UJRN/VKhnuvs 2014 4 10

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

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

94. 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.

95. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя. 2020. № 1. С. 102-109.

96. Пушак Я.Я., Марченко О.М. Проблемні аспекти запобігання та протидії кіберзлочинності в Укра- їні. Економічна та інформаційна безпека: проблеми та перспективи: матер. Міжнар. наук.-практ. конф. (м. Дніпро, 27 квітня 2021 р.). Дніпро, 2021. С. 173–176.

97. Кравцова М.О., Литвинов О.М. Запобігання кі- берзлочинності в Україні. Харків : Панов, 2019. 210 с.

98. Про затвердження Положення про Річні національні програми під егідою Комісії Україна НАТО: Указ Президента України від 24.02.21 р. № 72/2021. URL: https://www.president. gov.ua/documents/722021-36825

99. Нікулеско Д. Кібербезпека: вразливі моменти. Юридична газета online. 2019. URL: https://yur-gazeta. com/publications/practice/inshe/kiberbezpeka-vrazlivi- momenti.html

100. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. Інформація і право. 2021. No 1 (28). С. 118–128.

101. Про проведення парламентських слухань тему: "Кібербезпека, критична на інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення": Постанова Верховної Ради України від 04.02.20 р. № 500. URL: https://zakon.rada.gov.ua/laws/show/500-20#Text.