Шифр: **«CYBERCRIMES»**

Назва роботи: **«МІЖНАРОДНО-ПРАВОВЕ СПІВРОБІТНИЦТВО ДЕРЖАВ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ»**

Зміст

Вступ

Актуальність проблеми. Науково-технічний прогрес та розвиток інформаційних технологій посприяв змінам у суспільних відносинах. Як наслідок, взаємодії між суб'єктами суспільства стали неможливими без продуктів інформаційних технологій, а сфера їх застосування так розширилась, що на сьогодні важко уявити вид діяльності, де б не застосовувались технологічні пристрої та Інтернет. З кожним днем ми стаємо все більше залежними від IT інфраструктури. Разом з цим, зі зростанням соціальної значущості інформації та її безпеки, виникають нові виклики, спричинені суспільною небезпечністю неправомірних діянь у сфері інформаційних відносин.

Традиційне законодавство держав не було написане з урахуванням особливостей злочинів, що здійснюються у кіберпросторі. Основою проблемою в цьому відношенні стала складність застосування існуючих норм кримінального права до кіберзлочинів. Однак, слід зазначити, що разом із розвитком суспільства та технологій, характер злочинів та їх прояв також набрали нових форм. Кіберпростір став щоденними реаліями в 90-х роках, але розвиток кримінального законодавства не набув таких швидкостей. Це викликало потребу нових, чітко визначених, специфічних складів правопорушень в кримінальному законі, які б могли б забезпечити захист прав та законних інтересів користувачів кіберпростору від неправомірних посягань. Відповідно до досліджень американської компанії Броумім, що спеціалізується на розробці систем захисту і аналізу шкідливого програмного забезпечення, дохід із кіберзлочинності щорічно становить близько 1.5 трильйона доларів США (див. додаток).

В сучасному глобалізованому світі існує об'єктивна необхідність співробітництва держав у сфері боротьби з кіберзлочинністю та однорідності норм кримінального права у цій сфері. Така необхідність спричинена інтернаціональним характером кіберзлочинів, складністю визначення місця виконання такого злочину, можливість здійснення кіберзлочинів, залучивши

ЕОМ з місцезнаходженням у різних країнах (DDoS атаки) та організованою кіберзлочинністю. В цьому контексті актуальним є питання розвитку міжнародно-правового регулювання, спрямованого на боротьбу та превенцію кіберзлочинності, розробка на міжнародно-правовому рівні мінімальних стандартів, спрямованих на гармонізацію кримінального законодавства держав з метою уможливлення покарання за злочини, вчинені у кіберпросторі або з його використанням, запобіганню таким злочинам, їх розслідуванню та притягненню винних осіб до відповідальності. Крім того, оскільки кіберзлочини превалюють як злочини транснаціонального характеру, держави не здатні захистити свій правопорядок без взаємодії із іншими учасниками міжнародних відносин. Саме це створює об'єктивну необхідність міжнародно-правового регулювання у цьому контексті.

Важливим, у цьому аспекті, є зміст поняття кіберзлочину, оскільки він зумовлює рамки співробітництва держав у боротьбі з кіберзлочинністю. Крім цього, необхідним є встановлення механізмів боротьби з кіберзлочинності на міжнародному та регіональному рівні, оскільки саме їх ефективність визначає можливості держав співпрацювати у цій сфері.

Вивченням питанням комп'ютерних злочинів займались такі вчені, як О. Амелін, Д. Азаров та М. Крачевських. Такі ж вчені, як Ш.Шольберг, З. Гернауті, Ф. Калдероні присвятили свої праці питанням кіберзлочинності в контексі міжнародно-правового регулювання.

Мета і завдання дослідження. *Метою роботи* є аналіз міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю та імплементації Україною міжнародно-правових норм у цій сфері.

Досягнення зазначеної мети зумовило необхідність вирішення таких завдань: дослідити генезис міжнародно-правового регулювання боротьби з кіберзлочинністю; проаналізувати поняття та ознаки кіберзлочину у міжнародному праві; виявити міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні; визначити міжнародно-правовий механізм боротьби з кіберзлочинністю на регіональному рівні; проаналізувати

ступінь імплементації Україною міжнародно-правових норм у сфері боротьби з кіберзлочинністю, виявити потреби у вдосконаленні відповідного законодавства.

Об'єкт дослідження. Об'єктом дослідження є міжнародні правовідносини у сфері боротьби з кіберзлочинністю.

*Предмет дослідження***.** Предметом дослідження є міжнародно-правове співробітництво держав у боротьбі з кіберзлочинністю.

Методи дослідження*:* Під час дослідження було використано загальні та спеціальні методи. Загальними методами наукового пізнання, що було застосовано, є індукція, за допомогою якої зроблено висновок про наявність та характер міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю, формально-логічний метод, який дав змогу класифікувати види кіберзлочинів у міжнародному праві, та аналіз, з використанням якого було встановлено характер міжнародно-правового співробітництва держав у боротьбі з кіберзлочинності шляхом їх участі в регіональних конвенціях та діяльності в регіональних міжурядових організаціях. Також, у роботі використано спеціально-юридичні методи дослідження: становлення та розвиток міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю було досліджено за допомогою історико-правового методу, порівняння положень регіональних конвенцій про кіберзлочинність, а також рішень міжнародних організацій – порівняльно-правового, встановлення змісту міжнародно-правового звичаю щодо поняття кіберзлочину – формально-юридичного методу пізнання.

Перелік умовних скорочень

1. CIRT - Команда з реагування на комп’ютерні інциденти;
2. C-PROC - Офіс програми з кіберзлочинності при Раді Європи;
3. DDoS – (distributed) denial-of-service attack. Атака на відмову в обслуговування - напад на комп’ютерну систему з наміром зробити комп’ютерні ресурси недоступними користувачам, для яких комп’ютерна система була призначена. Атака зроблена з великої кількості комп’ютерів одночасно;
4. DoS denial-of-service attack. Атака на відмову в обслуговуванні - напад на комп’ютерну систему з наміром зробити комп’ютерні ресурси недоступними користувачам, для яких комп’ютерна система була призначена;
5. GCA – Global Cybersecurity Agenda (Глобальний план дій щодо забезпечення кібербезпеки);
6. REMJA - Зустрічі міністрів юстиції або інших міністрів або генеральних прокурорів американських держав при Організації американських держав;
7. SPSG - Група з безпеки та розвитку телекомунікацій та інформації при Організації Азійсько-Тихоокеанського економічного співробітництва;
8. SRI International – Scientific Research Institute. Американський неприбутковий науково-дослідницький інститут;
9. ATEC - Організація Азійсько-Тихоокеанського економічного співробітництва;
10. ЕОМ – електронно-обчислювальні машини;
11. ІКТ –інформаційно-комунікаційні технології;
12. ЛАД – Ліга арабських держав;
13. МСЕ – Міжнародний союз електрозв’язку;
14. ОАД – Організація американських держав;
15. ОЕСР – Організація економічного співробітництва та розвитку;
16. ООН ГУЕ - Група урядових експертів з питань розвитку сфери інформації та телекомунікації в контексті міжнародної безпеки;
17. РЄ – Рада Європи.

Розділ 1. Загальна характеристика міжнародного правової боротьби з кіберзлочинністю.

1.1. Становлення та розвиток міжнародно-правового регулювання боротьби з кіберзлочинністю.

Наприкінці 20-го століття використання мережі Інтернет тільки почало набирати швидких темпів. Тим не менш, можливість здійснення злочинів не залишилась поза увагою юридичної науки. Роботу над правовою концепцією кіберзлочину почав Донн Б. Паркер (США), який ще в 1970-х був залучений до дослідження понять кіберзлочину та кібербезпеки і став одним із основних розробників базового федерального керівництва для застосування права в США: «Комп'ютерні злочини – Керівництво для кримінальної юстиції» - 1979. Невдовзі це керівництво стало своєрідною енциклопедією із застосування права навіть поза межами США. Іншими американськими науковцями, що в той час працювали над концепцією кіберзлочину є Аугуст Беквейс та Джей Блуумбекер [1].

Крім представників США, на той час були й інші науковці, академічним інтересом яких була кіберзлочинність. Штайн Шольберг – норвезький прокурор – працював в Інтерполі з 1979 року, розроблявши концепцію цього нового феномену. В Німеччині професор Університету в Фрайбурзі Урліх Зібер був залучений до роботи багатьох міжнародних орагнізацій, таких як ОЕСР та ООН[2]. Нідерландський науковець Х.В.К. Касперсен, який пізніше став «батьком» Конвенції з боротьби з кіберзлочинністю 2001 року, почав її розробку ще в 1997 році [3].

Першим кроком міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю стала Конференція з кримінологічних аспектів економічних злочинів у Страсбурзі в 1976 році. Там було представлено декілька категорій кіберзлочинів [4].

Інтерпол

Першою міжнародної організацією, що апелювала саме до поняття кіберзлочину став Інтерпол (Конференція в Парижі 1979 році) [1]. Під час

презентації на тему комп'ютерного шахрайства було зазначено: «Природа комп'ютерного злочину є міжнародною, оскільки комунікація між різними державами здійснюється через телефони, супутники і т.д. Міжнародні організації, включно з Інтерполом, повинні приділяти цьому більше уваги».

Держави-учасниці Інтерполу взяли участь в опитуванні з питань кіберзлочинів рамках Першого навчального семінару Інтерполу з питань розслідування комп'ютерних злочинів в Парижі 7-11 грудня 1981 року. Це опитування дало можливість виявити прогалини в законодавстві з питань комп'ютерних злочинів, які потребують удосконалення правового регулювання. Це стало першим кроком у гармонізації кримінального законодавства у сфері кіберзлочинності державами світу[1].

ОЕСР

В 1982 році в Парижі ОЕСР вирішила створити комітет експертів з метою розглянути концепцію комп'ютерних злочинів та проаналізувати потребу реформування кримінальних законів. Результатом роботи комітету став «Аналіз політики ОЕСР з юридичних питань» 1986. Цей Аналіз зазначав:

«Відповідно до активізації комп'ютерної злочинності міжнародного характеру, було виявлено важливі питання, які потребують міжнародного співробітництва щодо контролю такої активності та боротьби із незаконними діяннями. Держави-учасниці повинні самі визначити межі, до яких покарання відповідні діяння повинні бути передбачені в кримінальному законодавстві».

Крім того, було визначено перелік діянь, за принципом спільного знаменника відповідно до концепцій, які були представлені державами-учасницями. У такий перелік входили: комп'ютерне шахрайство; комп'ютерна підробка документів; шкода, завдана комп'ютерним даним та програмам; неавторизоване посягання на захищені комп'ютерні програми і неавторизований доступ до або перехоплення комп'ютерних систем [1].

Рада Європи

В 1985 році Рада Європи призначена комітет експертів з метою розгляду комп'ютерних злочинів. Було розроблено рекомендації для національних законодавців, щодо виключно злочинів міжнародного характеру (Рекомендація № R (89) 9 – 1989 року) [4]. Ця рекомендація включала основний рекомендований список комп'ютерних злочинів та факультативний список.

Крім того, 11 вересня 1995 року Радою Європи було прийнято інші Рекомендації, які стосувались питання процесуального права в рамках інформаційних технологій. Ці Рекомендації налічували 7 розділів: розшук і затримання; технологічне спостереження; зобов'язання зі співробітництва органами розслідування; електронні докази; використання encryption; дослідження; статистика та завчання; міжнародне співробітництво [5].

ООН

Генеральна Асамблея ООН прийняла ряд резолюцій, найважливішими серед яких є Резолюція Генеральної Асамблеї 55/63 від 4 грудня 2000 року[6] і 56/121 від 19 грудня 2001 року з «Боротьби із зловживанням використання інформаційних технологій кримінального характеру». Відповідно до Резолюції Генеральної Асамблеї 55/63 від 4 грудня 2000 року:

« а) Державам повинні вжити заходів задля того, щоб їх законодавство і його застосування криміналізували та унеможливили зловживання інформаційними технологіями; б) Правові системи повинні захищати конфіденційність, цілісність даних та комп'ютерних систем, забезпечувати караність незаконних діянь».

Відповідно до Резолюції Генеральної Асамблеї 56/121 від 19 грудня 2001 року: *«Держави-учасниці, під час удосконалення власного законодавства, політики та діяльності з боротьби з кримінальним зловживанням інформаційними технологіями, зобов'язуються належним чином взяти до уваги розробки Комісії із запобігання злочинності та кримінального правосуддя, а також інших міжнародних та регіональних організацій»*[7].

1.2. Поняття та ознаки кіберзлочину в міжнародному праві

Визначення поняття та ознак кіберзлочину в міжнародному праві є особливо важливим для розуміння характеру співробітництва держав у сфері боротьби з кіберзлочинністю, адже це дає можливість встановити напрямки та окреслити рамки співробітництва, що здійснюється державами, а також дослідити механізми такого співробітництва.

В міжнародному праві не існує нормативно закріпленого визначення змісту поняття кіберзлочину на універсальному рівні, тому пошуки його формулювання повинні бути здійснені в актах м'якого права, регіональних джерелах, правовій доктрині, а також актах національного законодавства держав. Існує декілька підходів до визначення кіберзлочину. Метою цього розділу є формулювання визначних для кіберзлочину особливостей, які є характерними для усіх практик, що використовуються суб'єктами міжнародного права.

Одним з перших поняття кіберзлочину сформулював Донн Б. Паркер у праці «Комп'ютерні злочини – Керівництво для кримінальної юстиції» в 1979 році. Згідно з цим визначенням: «Злочини, пов'язані із використанням комп'ютера, - це будь-які порушення кримінального законодавства, які здійсненні з використанням знань у сфері комп'ютерних технологій для проникнення в них [у технології], їх дослідження або інших незаконних дій»[8]. Хоча таке визначення є досить широким, воно відповідає потребам того часу відносно характеру розвитку інформаційних технологій і кіберзлочинності.

Відмінним за формулюванням, але тотожним за змістом є визначення, сформульоване в Рекомендації № R (89) 9 – 1989 року, прийнятої Радою Європи, відповідно до якого: «ІТ злочини включають усі злочини, розслідування яких вимагає вилучення органами розслідування інформації, яка обробляється у комп'ютерних системах або передається через неї, або [вилучення] електронних систем обробки даних»[4]. Таке визначення відображає функціональний підхід.

На противагу, визначення, що використовувалось для робочий цілей ОЕСР у той час, було більш вузьким за своїм змістом: «Злочин, пов'язаний з використанням комп'ютера – це будь-яка незаконна, суспільно небезпечна, неправомірна поведінка щодо автоматичної обробки та передачі даних»[1].

При порівнянні цих визначень можна зробити висновок, що вже в той час сформувалось 2 основних підходи до визначення кіберзлочину:

– Кіберзлочин у вузькому значенні – злочини, у яких кіберпростір є об'єктом правопорушення (DoS, DDoS та ін.);

– Кіберзлочин у широкому значенні – злочини, у яких кіберпростір є об'єктом правопорушення або/і методом його вчинення (наприклад, розповсюдження дитячої порнографії та ін.)

Із розвитком міжнародного права та національного права держав, перевагу отримало широке визначення. Такий висновок можна зробити, проаналізувавши підходи до встановлення кола злочинів, які слід кваліфікувати кіберзлочинами, оскільки співробітництво держав охоплює обидва аспекти. Однак необхідно зазначити, що саме злочини, у яких кіберпростір є об'єктом правопорушення, потребують особливої уваги, оскільки такі правопорушення увійшли в кримінальне законодавство держав. Саме тому, одним із напрямів міжнародного співробітництва є розробка мінімальних стандартів щодо включення відповідних норм та їх застосування державами.

Міжнародні організації у резолюціях та рекомендаціях, як правило, уникали нормативного закріплення визначення кіберзлочину. На нашу думку, для цього існує декілька підстав: по-перше, вже з початку XX століття розвиток технологій набрав таких обертів, що з'явився ризик створення статичного визначення, яке б не змогло увібрати в себе ознаки тих злочинів, які ще не були відомі світові, тим самим, залишивши такі діяння поза правовим полем; по-друге, усі держави були і залишаються на різних стадіях імплементації міжнародно-правових стандартів з боротьби із кіберзлочинністю, відповідно, існували б труднощі імплементації такого визначення у національне законодавство. Саме тому визначення поняття кіберзлочину та встановлення

кола діянь, що кваліфікуватимуться як кіберзлочин – це прерогатива національного права.

Така думка знайшла своє вираження у висновках Комісії ООН із попередження злочинності та кримінального правосуддя (Відень, 2018): «Держави-члени [ООН] повинні вжити таких заходів, щоб їхнє законодавство щодо кіберзлочинності відповідало вимогам часу, зважаючи на майбутній розвиток технологій. З цією метою необхідно скасувати нормативні акти, формулювання яких є технологічно нейтральними, та криміналізувати не способи вчинення злочину, а діяння, яке слід вважати протиправним»[9].

Проте, міжнародне співробітництво держав у боротьбі з кіберзлочинністю було б не можливим, без виокремлення кола питань, які становлять його предмет. Міжнародні організації, розробляючи рішення, висновки та рекомендації, як правило, встановлювали перелік конкретних злочинів, що слід вважати кіберзлочинами.

Саме таких підхід був застосований у Конвенції Ради Європи про кіберзлочинність від 2001 року[10]. Відповідно до положень Конвенції кіберзлочини класифікуються як:

- правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями;
- правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами.
- правопорушення, пов'язані із змістом, зокрема, правопорушення, пов'язані з дитячою порнографією
- правопорушення, пов'язані з порушенням авторських та суміжних прав.

Таким ж напрям обрала ЛАД у Арабській конвенції з боротьби проти злочинів у сфері інформаційних технологій від 2010 року[11]. Відповідно до цієї Конвенції, держави-члени ЛАД беруть на себе зобов'язання криміналізувати такі види злочинів: злочини у сфері незаконного доступу до даних; злочини у сфері незаконного перехоплення даних; злочини проти

цілісності даних; злочини у сфері незаконного використання засобів інформаційних технологій; підробка; шахрайство; злочини, пов’язані з порнографією; злочини проти приватного життя; тероризм, вчинений за допомоги інформаційних технологій; злочини у сфері організованої злочинності, вчинені з використанням інформаційних технологій.

При порівняльному аналізі можна встановити, що різні регіональні конвенції до питання протидії кіберзлочинності відносять правопорушення одного ж характеру. Це дає нам можливість підтвердити аргумент про існування єдності розуміння поняття кіберзлочину.

Також, для встановлення змісту поняття кіберзлочин необхідно розглянути законодавство держав у сфері боротьби з кіберзлочиністю. Загалом існує 2 підходи, які були використані державами в метою доповнення законодавства: прийняття нормативно-правових актів та доповнення або внесення змін до існуючих. Наприклад, Кримінальний Кодекс Австрії був доповнений статтями, що передбачають покарання за такі діяння: незаконний доступ до комп’ютерних систем, перехоплення даних, шкода даним або комп’ютерним системам, підробка комп’ютерних даних та ін. Кримінальний кодекс Данії, до прикладу, крім вищезгаданих злочинів, також відокремлює злочини, пов’язані з підробленими електронними грошима, незаконне використання та створення платіжної інформації, що ідентифікує іншу особу, а також номерів платіжних карт. Варто зауважити, що такі норми є активними і вони використовуються органами влади у сфері, а також судами [12]. Крім того, відповідно до Закону Пакистану про запобігання електронним злочинам від 2016, прославлення злочину тероризму або особи, що засуджена за вчинення тероризму, також є кіберзлочином (визначення терміну «прославлення» надано у цьому акті відповідно) [13].

У Кримінальному кодексі України в редакції 5 квітня 2001 року [14] було відведено окремий розділ (Розділ XVI) злочинам у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Варто зазначити, що донедавна терміни

«кіберзлочинність», «кібербезпека» та «кіберзлочин» були відсутні як у законодавстві, так і в науці кримінального права України.

З набуттям чинності Закону України «Про основні заходи забезпечення кібербезпеки України» від 05.10.2017 [15] (набув чинності 5.05.2018) було заповнено прогалину в українському праві, що полягала у відсутності законодавчого закріплення поняття. Відповідно до цього закону: *Кіберзлочин* (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Пропонуємо розглянути визначення, запропоноване Європейським центром з боротьби з кіберзлочинністю (у складі Європолу) в публікації *Організована злочинність. Оцінка загроз 2017*: «Кіберзлочин можна визначити як будь-який злочин, що може бути вчинений тільки за умови використання комп'ютерів, комп'ютерних мереж або інших форм інформаційно-телекомунікаційних технологій» [16]. Хоча таке формулювання є досить абстрактним, на нашу думку, воно охоплює ознаки кіберзлочинів, а також воно є достатньо широким, тим самим передбачуючи можливість виникнення нових видів кіберзлочинів, досі не відомих суб'єктам міжнародного права, національним законодавцям та кіберсвіту загалом.

Хоча універсальне формулювання визначення відсутнє, практика суб'єктів міжнародного та національного права у цьому контексті дає нам підстави вважати, що такий підхід закріплений міжнародно-правовим звичаєм. Відповідно до О.В. Буткевича: «Для підтвердження наявності міжнародного звичаю, як правило, вказують на три головні фактори: а) міжнародна практика (прецеденти); б) opinio juris sive necessatis — думка, що визнає цю практику (прецеденти) за юридичну норму; в) фактор часу (тривалість застосування)» [14, с. 121].

На нашу думку, усе вищезазначене підтверджує існування міжнародно-правового звичаю щодо визначення кіберзлочину, оскільки:

– Співробітництво держав у сфері кіберзлочинності, що охоплює окремий перелік питань, а також наявність міжнародних договорів та актів міжнародних організацій, в яких кіберзлочин позиціонується як особливий вид злочину, що володіє специфічними ознаками, є підтвердженням міжнародної практики щодо змісту визначення кіберзлочину в міжнародному праві.

– Характеристика поняття кіберзлочину, визначення сфер та напрямів співробітництва між суб'єктами міжнародного права у сфері боротьби з кіберзлочинності, а також передбачення національним законодавством держав норм, що регулюють діяльність у кіберпросторі, а також використання таких норм їх органами свідчить про визнання такої практики за юридичну норму (opinio juris sive necessatis).

– Фактор часу для існування визначення кіберзлочину у звичаєвому праві має власні характерні особливості. Як вже зазначалось, увага суб'єктів міжнародного права до кіберзлочинів почала розвиватись ще на початку 80-тих років, а в 2001 вже було прийнято першу регіональну конвенцію. Тому, на нашу думку, в час, коли інформаційні технології розвиваються у надшвидкісному темпі, а разом з ними зростають й кіберзагрози, майже 40 років практики свідчить про тривалість її застосування.

Отже, відповідно до міжнародного звичаю, *кіберзлочин* – це протиправне винне діяння, що здійснюється в кіберпросторі або з його використанням, та за яке передбачене покарання національним кримінальним законом або міжнародним договором, згоду на чинність якого виражено відповідно до національного права держави.

На нашу думку, існування визначення кіберзлочину в міжнародному праві у формі міжнародного звичаю має позитивний характер, оскільки це забезпечує динамічність такого визначення з одного боку, та його статичність з іншого, оскільки воно передбачатиме можливість виникнення нових відносин, але й не створюватиме потребу в правотворчості договірного характеру у разі неможливості його застосування.

Розділ 2. Міжнародно-правовий механізм боротьби з кіберзлочинністю.

2.1. Міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні.

На сьогодні боротьба з кібербезпека є актуальним питанням для усіх членів світового співтовариства. Кібезлочинність, поряд з *кібертероризмом, кібервійною* та іншою неправомірною *кібердіяльністю,* створює загрозу для світової кібербезпеки. Боротьба з кіберзлочинністю була б не можлива без співпраці на міжнародно-правовому рівні, оскільки вона вимагає не тільки гармонізацію законодавства держав у цій сфері, а й не може існувати без взаємодій національних органів між собою та із міжнародними структурами. Вони, в свою чергу, розробляють документи та навіть створюють підрозділи або структури з метою забезпечення кібербезпеки, в тому числі шляхом попередження кіберзлочинів, розробки заходів щодо їх ефективного розслідування та фасилітації процесу притягнення винних осіб до відповідальності. У цьому розділі буде розглянуто міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні та проаналізовано наявні проблеми в контексті міжнародно-правового регулювання співпраці суб'єктів міжнародного права на універсальному рівні.

ООН

Діяльність ООН щодо боротьби з кіберзлочинністю на сьогодні представлена рядом резолюцій, серед яких слід зосередити увагу на Резолюціях ГА ООН 55/63 від 2000 року та 56/112 від 2001 року "Боротьба зі злочинним використанням інформаційних технологій". У Резолюції 55/63 наголошується:

"1.Держави повинні вжити таких заходів, щоб їх законодавство та практика зробили неможливим уникнути покарання тими, хто злочинно використовує інформаційні технології

2. Співпраця держав щодо розслідування випадків злочинного використання інформаційних технологій міжнародного характеру та

переслідування за такі злочини повинна відбуватись шляхом координації з боку усіх заінтересованих держав"[6].

Відповідно до Резолюції 56/112, ООН:

"1. закликає держав-членів, під час розробки національних законів, політики і практики щодо боротьби зі злочинним використанням інформаційних технологій належним чином враховувати роботу і досягнення Комісії з попередження злочинності та кримінального правосуддя, а також інших міжнародних і регіональних організацій[7].

Також важливе значення має Резолюція 65/230 [18], якою Генеральна Асамблея затвердила "Глобальну програму з кіберзлочинності " та ініціювала створення *Міжнародної експертної групи відкритого складу з метою проведення всестороннього дослідження питання кіберзлочинності.* Метою такого дослідження є збір та обмін інформацією про національне законодавство держав, найкращі практики, технічну допомогу та міжнародну співпрацю, беручи до уваги можливі способи зміцнення існуючих та впровадження нових законодавчих заходів або іншим способів боротьби із кіберзлочинністю. У квітні 2018 року у Відні відбулась вже 4 сесія міжнародної експертної групи, в результаті якої було створено Рекомендації, у яких, між іншим, наголошується: *"Формулюючи положення законів та політику, держави-учасниці повинні враховувати потребу в балансі між захистом прав людини, з одного боку, та питанням державної безпеки, публічного порядку, та законних прав третіх осіб з іншого"* [9]

Іншою структурою ООН, діяльність якої пов'язана із співробітництвом щодо неправомірного використання кіберпростору, є ООН ГУЕ - *Група урядових експертів з питань розвитку сфери інформації та телекомунікації в контексті міжнародної безпеки.* Це робоча група під мандатом ООН, діяльність якої зосереджена на інформаційній безпеці. Головними досягненнями цієї робочої групи є впровадження глобальної програми з кібербезпеки та виклад того, як принципи міжнародного публічного права

застосовуються до кіберпростору. Серед питань, які належать до відання групи є питання:

- які ознаки кваліфікують кібератаку як “використання сили” і/або “збройного нападу”;
- чи є застосування існуючих норм міжнародного права в контексті кібезлочинності, чи існує необхідність прийняття нових норм?
- чи є кіберпростір окремою ланкою міжнародних відносин?
- як застосовуються норми міжнародно-правової відповідальності держав у випадку міжнародно кібератаки? [19]

Потрібно зауважити, що така незаконна діяльність у кіберпросторі вже не може кваліфікуватись як кіберзлочинність, оскільки в питаннях, що вивчає ООН ГУЕ, кібератаки ініціюються державами (наприклад, кібератаки на об’єкти критичної інфраструктури). Агресія в кіберпросторі створює нові виклики для міжнародного публічного права. Крім того, складним залишається питання доведення причетності держави до кібератаки, оскільки в багатьох випадках вони здійснюються приватними особами або організаціями. Варто також зазначити, що ОНН ГУЕ - це не єдина організація, яка зосереджує увагу на цих питаннях: Об’єднаний центр передових технологій з кібероборони НАТО спричинився до створення “Талліннського керівництва з питань застосування міжнародного публічного права до кібердій 2.0” від 2017 року, розробленого 19 експертами з міжнародного права. Це керівництво є другим виданням від редакції 2013 року. Керівництво складається з чотирьох частин, які присвячені співвідношенню загальної частини міжнародного права та кіберпростору; спеціальних режимів міжнародного права та кіберпростору; міжнародного миру та безпеки і діяльності в кіберпросторі; праву збройних “кіберконфліктів”.

МСЕ

Міжнародний союз електрозв’язку є ще одною організацію, до напрямів діяльності якої входить боротьба з кіберзлочинністю. В 2007 році Генеральний секретар МСЕ запустив проект під назвою Global Cybersecurity Agenda (GCA),

яким було створено засади міжнародного співробітництва, необхідного у час, коли відбувається швидке збільшення загроз кібезбезпеці. GCA пропонує державам рекомендації щодо зміцнення кібербезпеки в інформаційному суспільстві.[1] Необхідно зазначити, що на сьогодні МСЕ є універсальною міжнародною організацію, яка найбільш активно займається питанням створення стандартів кібербезпеки. Вона активно сприяє гармонізації національного законодавства через проект *Борючись із кіберзлочинністю: Інструменти та можливості для країн з перехідною економікою (*розроблений спільно з Управлінням ООН з наркотиків та злочинності). Цей проект є Інтернет-платформою, з відкритими ресурсами та публікаціями, що можуть слугувати для роботи осіб, що визначають політику кібербезпеки, законодавців, прокурорів та слідчих, громадянського суспільства в контексті створення середовища для боротьби з кіберзлочинністю. Платформа, в свою чергу, класифікує ресурси у три розділи: узагальнення міжнародної практики щодо боротьби з кіберзлочинністю; розробка інструментів, спрямованих на оцінку державою своїх правових можливостей боротьби із кіберзлочинністю та визначення пріоритетів реформування; запровадження "Віртуальної бібліотеки", що систематизує матеріали проектів організацій-партнерів МСЕ (серед яких є міжнародні міжурядові, а також неурядові організації)[20].

Також. наступним проектом МСЕ є публікація *Розуміння кіберзлочину: явище, загрози та правові заходи.* Ця публікація спрямована допомогти державам у розумінні зв'язків кібербезпеки та використання ІКТ, а також кіберзлочинності. Також, цей проект допомагає країнам, що розвиваються у розумінні викликів, пов'язаних із зростанням кіберзагроз та сприяє в оцінці поточного стану відповідного законодавства або впровадження такого законодавства у випадках, коли воно ще не є імплементованим[21].

Також, МСЕ сприяє створенню ефективних інституційних механізмів, які є необхідними у боротьбі та запобіганню кіберзлочинності. На національному рівні державами створено спеціальні структури - CIRT (Команди з питань реагування на комп'ютерні інциденти). Ці структури вже

створені в 103 країнах. Союз координує діяльність Команд та забезпечує обмін необхідною юридичної та технічною інформацією[22].

Крім того, МСЕ щорічно публікує Глобальний індекс кібербезпеки (Global Cybersecurity Index), який покликаний оцінити діяльність держав щодо їх заходів у контексті кібербезпеки. Індекс враховує показники щодо п’яти основних аспектів забезпечення кібербезпеки: правових заходів, технічних заходів, організаційних заходів, впровадження можливостей та рівня співпраці. Дана публікація аналізує поточну ситуацію щодо кібербезпеки як на універсальному рівні, так і відповідно до регіональних показників[23].

Проект конвенції з кіберзлочинності

На нашу думку, очевидною є необхідність укладення універсального міжнародного договору, який би уніфікував стандарти політики держав у контексті кібербезпеки, а також сприяв би гармонізації матеріального та, більш важливо, процесуального права в контексті боротьби з кіберзлочинністю. Як вже раніше було зазначено, міжнародний характер кіберзлочинів безумовно викликає необхідність такої гармонізації. Оскільки питання віднесено до сфери регулювання національним правом, уніфікація стандартів можлива тільки через співробітництво в рамках міжнародних організацій. На сьогодні, питання кібербезпеки є дуже актуальним, тому багато організацій публічного та приватного, міжнародного та національного спрямування займаються питанням кібербезпеки. Також, здійснюється міжнародне співробітництво щодо обміну інформацією не тільки правового, а й технічного характеру, створюються центри запобігання кіберзлочинам і т.п. Проте таке співробітництво. на жаль, має дисперсний характер. Тому, укладення універсального договору могло б створити умови для більш продуктивного співробітництва та залучити ще більше держав до такої діяльності.

Активну позицію щодо впровадження такого договору займає міжнародний експерт з питань кіберзлочинності Штайн Шольберг - суддя у відставці Спеціального апеляційного суду в Норвегії. Штайн Шольберг консультував багато міжнародних організацій (зокрема МСЕ, та Управління

ООН з наркотиків і злочинності, Інтерпол) з питань кіберзлочинів. Саме йому належить ініціатива розробки відповідної конвенції. Разом із професором Лозанського університету (Швейцарія) Золанжем Гернауті, Штайн Шольберг опублікував *Проект Женевської конвенції чи декларації з кіберпростору*[24] у 2016 році (далі - Женевська конвенція). Норми, правила та стандарти Женевської конвенції покликані уникнути фрагментарності та розбіжності регулювання та стати універсальною рамкової угодою щодо кіберпростору. Крім того, Женевська конвенція могла б допомогти сучасним національним та регіональним ініціативам уникнути дублювання діяльності та зміцнила б співробітництво між ними. Стандарти, запропоновані конвенцією, охоплюють наступні аспекти: стандарти заходів щодо міжнародної кібербезпеки; стандарти правових заходів; стандарти з міжнародного співробітництва та координації щодо розслідування кіберзлочинів - зокрема через Інтерпол; стандарти глобального співробітництва публічного та приватного-правового секторів; стандарти для організації Міжнародного кримінального суду чи трибуналу з кіберпростору[25].

Однак, на нашу думку, світова спільнота не готова до укладення Женевської конвенції, через наявність у ній деяких контроверсійних положень, зокрема ініціативи створення Міжнародного кримінального суду чи трибуналу з кіберпростору. Це передбачало б поширення юрисдикції ще одного міжнародного органу, що не є бажаним для всіх суб'єктів, оскільки інколи держави й самі використовують неправомірну діяльність в кіберпросторі як інструмент своєї зовнішньої та внутрішньої політики.

Крім того, оскільки зараз міжнародно-правове регулювання співробітництва щодо кіберпростору має здебільшого регіональний характер, враховано регіональні особливості правовідносин у контексті використання кіберпростору, впровадження кримінального та кримінально-процесуального законодавства, врахування вимог стандартів фундаментальних прав людини, рівень залученості ІКТ та фінансово-бюджетні можливості держав. Впровадження уніфікованих стандартів вимагає досягнення консенсусу із

спірних питань, що створює певні труднощі на сьогодні. Саме це, на нашу думку, є причиною відсутності універсального міжнародно-правового регулювання співробітництва з боротьби з кіберзлочинності шляхом укладення відповідної конвенції, хоча це , без сумніву, дало б позитивний результат.

2.2. Міжнародно-правовий механізм боротьби з кіберзлочинністю на регіональному рівні.

На сьогодні міжнародно-правове регулювання боротьби з кіберлочинності має, здебільшого, регіональний характер. Таке співробітництво, як правило, здійснюється державами під егідою міжнародних регіональних організацій, членами яких вони є. В останні роки прослідковується тенденція активізації взаємодій у цьому напрямку, шляхом укладення основоположних для цього питання регіональних угод, створюючи не тільки юридичні механізми боротьби з кіберзлочинністю, а й практичні, що втілюються в роботі спеціальних інституцій, робочих дослідницьких груп, контакт центрів та ін.

Організацією, що започаткувала міжнародно-правове співробітництво регіонального характеру, є Рада Європи. Конвенція Ради Європи про кіберзлочинність була підписана 23 листопада 2001 року на конференції в Будапешті і стала фундаментом боротьби з кіберзлочинністю, заклавши основи співробітництва, стандарти криміналізації кіберзлочинів та вимоги до процесуального права не тільки для країн-членів Ради Європи, а й усієї світової спільноти. Усі майбутні документи укладалися з огляду на положення конвенції, а деякі з них - з прямим посиланням на конвенцію. Наприклад, в Директиві ЄС 2013/40 про посягання на інформаційні системи [26]. Відповідно до преамбули (15): *«Нова стратегія повинна бути розроблена державами-членами і Комісією, беручи до уваги зміст Конвенції Ради Європи про кіберзлочинність від 2001 року. Ця Конвенція є юридичною основою для боротьби з кіберзлочинами, із посяганнями на інформаційні системи включно. Ця Директива побудована відповідно до Конвенції».*

Відповідно до даних від 9 грудня 2018 року, Конвенцію про кіберзлочинність підписали 62 країни (25 з яких не є членами РЄ, та ще 4

підписали, але не ратифікували) [27]. Це свідчить не тільки про якість самого договору, а також про бажання держав долучатись до співробітництва та впроваджувати у своє законодавство норми, які дадуть можливість ефективно здійснювати протидію кіберзлочинами та боротьби з ними.

Як вже раніше зазначалось, Конвенція з кіберзлочинності стала проривом у боротьбі із кіберзлочиністю. Саме вона задала напрямок для майбутньої універсалізації відповідних норм. Конвенція застосовує нейтральну щодо технологій юридичну техніку, і тому, відповідно, передбачає застосування як щодо сучасних правопорушень, так і до таких, що можуть виникнути в майбутньому із розвитком технологій [1].

Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [28] був прийнятий в 2003 році у Страсбурзі. Він доповнив перелік кіберзлочинів наступними діяннями: поширення расистського та ксенофобного матеріалу через комп'ютерні системи, погроза з расистських та ксенофобських мотивів, образа з расистських та ксенофобських мотивів, заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства. На сьогодні додатковий протокол ратифікували 31 держава, та ще 13 підписали.

Крім того, відповідно до статті 46 Конвенції було засновано Комітет з кіберзлочинності, метою якого є консультації щодо сприяння імплементації та ефективного застосування Конвенції, забезпечення обміну інформацією та впровадження майбутніх доповнень. В 2017 році Комітетом було прийняте рішення розробити проект Другого протоколу до Конвенції про кіберзлочинність, зокрема для вирішення таких категорій питань: заходи щодо ефективного взаємного співробітництва; заходи, що забезпечують безпосереднє співробітництво із провайдерами в інших юрисдикціях, задля запитів інформації щодо користувачів, збереження інформації та невідкладних запитів; більш точне формулювання та інтенсивніше забезпечення існуючих практик

щодо транскордонного доступу до даних; заходи, спрямовані на забезпечення захисту даних [29].

Більше того, при РЄ в Бухаресті, Румунія, діє Офіс програми з кіберзлочинності (C-PROC), завданням якого є допомога державам посилити їх юридичні механізми щодо відповіді загрозам кіберзлочинності та функціонування електронних доказів відповідно Конвенції з кіберзлочинності. Офіс займається реалізацією ряду проектів, диференційованих за регіональною ознакою, щоб більше ефективно виявити потреби правових систем та забезпечити необхідні консультації [30].

Наступною пропонуємо розглянути Лігу арабських держав. В грудні 2010 в рамках цієї організації було прийнято Арабську конвенцію з боротьби з кіберзлочинами [31] та набрала чинності в 2014. На сьогодні її ратифікували 8 держав-членів ЛАД. Головною метою конвенції є створення зобов'язань для її учасників щодо імплементації у їх національне право положень, які б криміналізували ряд кіберзлочинів, а так само впровадження процесуальних норм задля спрощення процесу переслідування за кіберзлочини та збирання електронних доказів. Конвенція також має розділ щодо налагодження співпраці між країнами-учасницями з боротьби з міжнародними кіберзлочинами. Арабська конвенція з боротьби з кіберзлочинами прямо не передбачає механізму правозастосування чи процедури вирішення суперечок.

Конвенція має ряд контроверсійних положень, зокрема таких, як ст. 21, яка вимагає більш жорсткого покарання за традиційні злочини, якщо вони були вчинені із застосуванням кіберпростору (на нашу думку, без об'єктивних на те причин). Крім того, стаття 21.1 передбачає покарання за розповсюдження порнографічних матеріалів, стаття 12.1 - розповсюдження ідей та принципів терористичних груп, стаття 15.4 - поширення релігійного фанатизму та інакомислення. Таким чином, можна зробити висновок про обмеження Конвенцією певних прав людини, зокрема права на свободу слова та віросповідання [32].

Африканський союз в 2011 році почав розробку Конвенції з кібербезпеки ще в 2011 році, метою якої було встановлення ефективної програми з кібербезпеки в Африці через впорядкування електронних транзакцій, захист персональних даних, заохочення до впровадження заходів із кібербезпеки, електронного врядування та боротьби з кіберзлочинністю. Однак, Африканська конвенція з кібербезпеки та захисту персональних даних була остаточно прийнята в 2014 році[33]. Стаття 29 надає перелік злочинів, передбачених конвенції. Однак, Африканська конвенція не передбачає більшості процесуальних норм, що містяться у Конвенції РЄ з кіберзлочинності 2001 року. Крім того, відмінністю є те, що Африканська конвенція криміналізує, в деяких випадках, не тільки закінчений злочин, а й замах на злочин.

Також, в жовтні 2018 року в рамках Африканської конвенції відбувся Перший африканський форум з боротьби з кіберзлочинністю. Серед розглянутих питань: політика з боротьби з кіберзлочинністю, національне законодавство в рамках регіональних та міжнародних стандартів, практика їх імплементації; міжнародна співпраця з боротьби з кіберзлочинності та відповідна реалізація заходів із забезпечення транскордонної передачі електронних злочинів; посилення роботи органів кримінальної юстиції через впровадження юридичних можливостей через відповідні програми, що діють на Африканському континенті [34].

Також існують інші форми міжнародно-правової співпраці з боротьби з кіберзлочинності. Хоча такі інструменти не є юридично-зобов'язальними, вони забезпечують співробітництво з практичної сторони. Зокрема, Організація Азійсько-Тихоокеанського економічного співробітництва в 2003 році започаткувала Проект з сприяння законодавству з кіберзлочинності та правозастосовчих заходів, метою якого є допомога державам регіону посилити їх юридичні можливості щодо боротьби із кіберзлочинами та заохочення розвитку законодавства щодо правозастосування та розслідування кіберзлочинів, задля ефективізації боротьби із кіберзлочинністю [35]. Крім

того, при АТЕС діє Група з безпеки та розвитку телекомунікацій та інформації (SPSG), яка сприяє безпеці кіберпростору та, inter alia, займається питаннями запобігання кіберзлочинності [36].

Іншою організацією, що реалізовує співпрацю такого типу є Організація американських держав. В її межах засновані спеціальні робочі групи та проект з назвою Міжамериканський портал співробітництва з боротьби з кіберзлочинністю. Завданням порталу є спростити співпрацю та обмін інформацією між компетентними органами держав ОАД у сфері боротьби з кіберзлочинністю, міжнародної співпраці щодо їх розслідування та переслідування за них [37].

Отже, регіональний механізм міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю представлений у двох форматах: через впровадження спільних заходів юридичного характеру відповідно до потреб конкретних регіонів, та через організацію роботи спеціальних інституцій, що здійснюють дослідження та координацію правового співробітництва держав, зокрема на регіональному рівні. Основні аспекти забезпечення боротьби з кіберзлочинністю, зокрема через впровадження матеріальних та регіональних норм до національного законодавства держав, характерні не всім регіонам. Хоча така співпраця враховує особливості правових систем держав-членів світової спільноти, вона не забезпечує універсалізації норм на міжнародному рівні, яка є необхідною з огляду на той факт, що кіберзлочини, у більшості форм їх вияву, не можна обмежити кордонами та юрисдикціями.

Також, універсалізація міжнародно-правового регулювання боротьби з кіберзлочинності посприяла б зменшенню випадків впровадження державами норм національного права, які б обмежували фундаментальні права людини.

Крім того, створення єдиного універсального міжнародно-правового механізму співробітництва з боротьби проти кіберзлочинності дало б можливість створити окрему спеціалізовану інституцію для процесуальних аспектів превенції та протидії кіберзлочинності, що дало б можливість

покращити вже існуючі форми співробітництва та залучити більше учасників до такої діяльності.

2.3. Імплементація Україною стандартів боротьби з кіберзлочинністю

Україна є учасником Конвенції про кіберзлочинність від 2001 року, яка, на сьогодні, є єдиним міжнародним договором, присвяченим питанням кіберзлочинності, що складає частину національного законодавства України. Комітет РЄ з питань кіберзлочинності, спільно з Європейським союзом, надає підтримку країнам Східного партнерства у сфері кіберзлочинності. У квітні 2016 року в Києві було відкрито проект «Кіберзлочинність. Східне партнерство III», що став третім етапом у наданні РЄ підтримки державам-учасницям проекту консультацій та рекомендацій щодо гармонізації законодавства у сфері кіберзлочинності відповідно до положень конвенції. Серед питань до обговорення були присутні питання чіткості та застосовності законодавства, послідовності та належної імплементації конвенції. Особлива увага спрямована на здійснення державами взаємної правової допомоги на стадіях досудового та судового розгляду. Крім того, стратегічно важливим Комітет на той час зосередив свою увагу на питанні доступу до електронних доказів у кримінальній юстиції. Також, було розроблено звіт щодо України про чинне законодавство у сфері кіберзлочинності від 3 листопада 2016 року[38], який висвітлив прогалини в законодавстві, встановив відповідність існуючих норм до положень Конвенції та проаналізував внесені законопроекти. Слід зазначити, що з моменту публікації звіту, було зроблено певні кроки для його удосконалення. Зокрема, законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів»[39] від 3.10.2017 до всіх цих процесуальних кодексів додано параграф під назвою «Електронні докази».

3-4 травня 2018 у Києві відбулась Четверте регіональне засідання з міжнародної співпраці з питань кіберзлочинності та електронних доказів. Там було представлено Переглянуту доповідь з питань міжнародного

співробітництва щодо боротьби з кіберзлочинністю в регіоні Східного партнерства від 2018 року[40]. Відповідно до доповіді: відділ Кіберполіції Національної поліції України забезпечує діяльність 24/7-контакт центру, опрацьовує тільки ті запити, що отримані ним від іноземних відділів поліції, шо стосуються питань кіберзлочинності та електронних доказів. Контакт центр здійснює співробітництво з питань розслідування кримінальних злочинів, комп'ютерними системами та забезпечує обмін оперативними даними (що не є доказами в кримінальному процесі). Відповідно до законодавства України, розгляд запитів щодо надання правової допомоги належить до компетенції центральних органів влади. Такий запит не може бути здійснено оперативно, оскільки центральні органи влади не забезпечені 24/7 контакт-центрами. Також, відсутній механізм обміну такими запитами між Службою Безпеки України та Національної Поліцією України.

Крім того, актуальними для вдосконалення українського законодавства залишаються наступні питання:

– термінове збереження визначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи;

– термінове збереження і часткове розкриття даних про рух інформації;

– порядок представлення комп'ютерних даних, якими особа володіє або контролює, і які зберігаються у комп'ютерній системі або на комп'ютерному носії інформації;

– надання повноважень компетентним органам для обшуку або подібного доступу до комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній та комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані; арештовувати або вчиняти подібні дії щодо комп'ютерних даних, до яких був здійснений доступ;

– збирання комп'ютерних даних про рух інформації у реальному масштабі часу.

Висновок

Отже, становлення та розвиток уявлення щодо змісту поняття кіберзлочину у міжнародному праві через діяльність юристів-науковців та суб'єктів міжнародного права ще в 70-х, і з ним зростає необхідність міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю.

Зміст поняття кіберзлочину закріплений міжнародно-правовим звичаєм, відповідно до якого *кіберзлочин* – це протиправне винне діяння, що здійснюється в кіберпросторі або з його використанням, та за яке передбачене покарання національним кримінальним законом або міжнародним договором, згоду на чинність якого виражено відповідно до національного права держави. Необхідність закріплення такого визначення міжнародно-правовим договором відсутня, оскільки, на нашу думку, існує багато переваг існування відповідного правового звичаю через поєднання у ньому статичності та динамічності. Крім того, класифікація кіберзлочинів відповідно до різних джерел міжнародного права, а саме міжнародних договорів та актів міжнародних міжурядових організацій, підтверджує тезу щодо стійкості та системності уявлень про зміст та характер кіберзлочину.

Міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні функціонує в рамках таких організацій, як ООН, МСЕ, Інтерпол та ін., які своїми актами сприяють співробітництву держав та встановлюють напрямки їх діяльності щодо імплементації міжнародно-правових стандартів криміналізації кіберзлочинів. На регіональному рівні співробітництво здійснюється у двох форматах: через впровадження спільних заходів юридичного характеру відповідно до потреб конкретних регіонів, та через організацію роботи спеціальних інституцій, що здійснюють дослідження та координацію правового співробітництва держав, зокрема на регіональному рівні. Успіхами регіонального співробітництва можна вважати підписання таких міжнародно-правових договорів, як Конвенція РЄ про кіберзлочинність, Африканська конвенція з кібербезпеки та захисту персональних даних та Арабська конвенція з боротьби з кіберзлочинами. Однак, на нашу думку,

укладення міжнародно-правового договору на універсальному рівні дало б можливість уніфікувати законодавство держав у сфері кіберзлочинів, що б полегшило співробітництво держав щодо виявлення кіберзагроз, попередження кіберзлочинів, їх розслідування та розкриття, зокрема шляхом обміну інформацією у формі електронних доказів в рамках міжнародної правової допомоги.

Україна є суб'єктом міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю, зокрема через участь у Конвенції РЄ про кіберзлочинність. В законодавство України імплементовано усі матеріальні норми, передбачені Конвенцією, однак деякі процесуальні аспекти потребують подальшої гармонізації. Крім того, в Україні діє 24/7 контакт-центр при відділі Кіберполіції Національної поліції України, який здійснює обмін цифровою інформацією із закордонними структурами.

Загалом, варто відзначити позитивні тенденції у міжнародно-правовому співробітництві держав у боротьбі з кіберзлочинністю. Із зростанням ролі кіберпростору в житті суспільства та відповідним збільшенням обсягу кіберзагроз, слід очікувати активізації такого співробітництва, розробки суб'єктами міжнародного права узагальнених принципів та впровадження удосконалених норм.

Список використаних джерел

1. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva [Електронний ресурс] / Stein Schjolberg. – 2008. – Режим доступу до ресурсу: http://cybercrimelaw.net/documents/cybercrime_history.pdf
2. Prof. Dr. Ulrich Sieber [Електронний ресурс] // Max-Planck-Institut für ausländisches und internationales Strafrecht – Режим доступу до ресурсу: https://www.mpicc.de/de/home/sieber.html
3. Council of Europe. Explanatory Report to the Convention on Cybercrime [Електронний ресурс] / Council of Europe // European Treaty Series - No. 185. – 23. – Режим доступу до ресурсу: https://rm.coe.int/16800cce5b.
4. Recommendation No. R (89) 9 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON COMPUTER-RELATED CRIME [Електронний ресурс] // Council of Europe. – 1989. – Режим доступу до ресурсу: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094
5. RECOMMENDATION No. R (95) 13 CONCERNING PROBLEMS OF CRIMINAL PROCEDURAL LAW CONNECTED WITH INFORMATION TECHNOLOGY [Електронний ресурс] // Council of Europe. – 1995. – Режим доступу до ресурсу: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76
6. Resolution 55/63. Combating the criminal misuse of information technologies [Електронний ресурс] // General Assembly of the United Nations. – 2000. – Режим доступу до ресурсу: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
7. Resolution 56/121. Combating the criminal misuse of information technologies [Електронний ресурс] // General Assembly of the United Nations. – 2001. – Режим доступу до ресурсу: http://undocs.org/A/RES/56/121

8. Parker D. Computer Crime: Criminal Justice Resource Manual [Електронний ресурс] / Donn B. Parker // u.s. Department of Justice National Institute of Justice Office of Justice Programs. – 1979. – Режим доступу до ресурсу: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf

9. Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018 [Електронний ресурс] // UN. Commission on Crime Prevention and Criminal Justice. – 2018. – Режим доступу до ресурсу: http://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/V1802315.pdf

10. Конвенція про кіберзлочинність від 23.11.2001 р. [Електронний документ] / Верховна Рада України : Законодавство. – 25.08.2012 р. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_575

11. Arab Convention on Combating Information Technology Offences [Електронний ресурс] // The League of Arab States. – 2010. – Режим доступу до ресурсу: http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences

12. Handbook of Legal Procedures of Computer and Network Misuse in EU Countries [Електронний ресурс] / [L. Valeri, G. Somers, N. Robinson та ін.] // The RAND Corporation. – 2006. – Режим доступу до ресурсу: https://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR337.pdf

13. The Prevention of Electronic Crimes Act [Електронний ресурс] // National Assembly of Pakistan. – 2016. – Режим доступу до ресурсу: http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

14. Кримінальний кодекс України: закон України від 5 квітня 2001 р. № 2341-III // Відомості Верховної Ради України. – 2001 – № 25-26, ст.131

15. Закон України «Про основні заходи забезпечення кібербезпеки України» від 05.10.2017 /Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.

[Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19

16. Internet organised crime threat assessment [Електронний ресурс] // European Cybercrime Centre. Europol. – 2017. – Режим доступу до ресурсу: https://www.europol.europa.eu/iocta/2017/index.html

17. Міжнародне право. Основи теорії: Підручник / За ред. В. Г. Буткевича. — К.: Либідь, 2002. — 121 с.

18. 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

19. The UN GGE - United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [Електронний ресурс] // United Nations – Режим доступу до ресурсу: https://dig.watch/processes/ungge

20. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. [Електронний ресурс] // ITU – Режим доступу до ресурсу: http://www.combattingcybercrime.org/

21. Understanding cybercrime: phenomena, challenges and legal response [Електронний ресурс] // ITU. – 2014. – Режим доступу до ресурсу: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf

22. National CIRT [Електронний ресурс] // ITU – Режим доступу до ресурсу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

23. Global Cybersecurity Index (GCI) 2017 [Електронний ресурс] // ITU. – 2017. – Режим доступу до ресурсу: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

24. VFAC Review No. 12 [Електронний ресурс] // Korean Institute of Criminology. – 12. – Режим доступу до ресурсу: https://eng.kic.re.kr/brdthm/boardthmView.do?srch_menu_nix=u23eHZq1&brd_id=BDIDX_88DG8kFqLCEhPR0f556FNc&srch_mu_lang=CDIDX00023

25. A Geneva Convention or Declaration for Cyberspace [Електронний ресурс] // Presentation at the WSIS Forum 2018 – Режим доступу до ресурсу: http://www.cybercrimelaw.net/documents/Presentation1.pdf

26. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [Електронний ресурс] // EUR-Lex. – 2013. – Режим доступу до ресурсу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

27. Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime [Електронний ресурс] // Council of Europe. – 9. – Режим доступу до ресурсу: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=j5hEAdZ2

28. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems [Електронний ресурс] // Council of Europe. – 2003. – Режим доступу до ресурсу: https://rm.coe.int/168008160f

29. 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

30. Cybercrime Programme Office (C-PROC) [Електронний ресурс] // Council of Europe – Режим доступу до ресурсу: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

31. Arab Treaty on Combating Cybercrime [Електронний ресурс] // Riyadh Al-Balushi. – 2015. – Режим доступу до ресурсу: http://www.riyadh.om/2015/arab-treaty-on-combating-cybercrime/.

32. Multilateral tracks to tackling cybercrime: an overview [Електронний ресурс] // Samuele Dominioni. – 16. – Режим доступу до ресурсу:

https://www.ispionline.it/en/pubblicazione/multilateral-tracks-tackling-cybercrime-overview-20962

33. African Convention on Cyber Security and Personal Data Protection [Електронний ресурс] // African Union. – 2014. – Режим доступу до ресурсу: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

34. The First African Forum on Cybercrime [Електронний ресурс] // African Union. – 8018. – Режим доступу до ресурсу: https://au.int/en/newsevents/20181016/first-african-forum-cybercrime.

35. Strengthening International Law Enforcement Cooperation to Prosecute Cyber Criminals, Hackers and Virus Authors [Електронний ресурс] // Asia-Pacific Economic Cooperation. – 2003. – Режим доступу до ресурсу: https://www.apec.org/Press/News-Releases/2003/0718_sin_strengthening_international_law.

36. 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.

37. 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.

38. 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

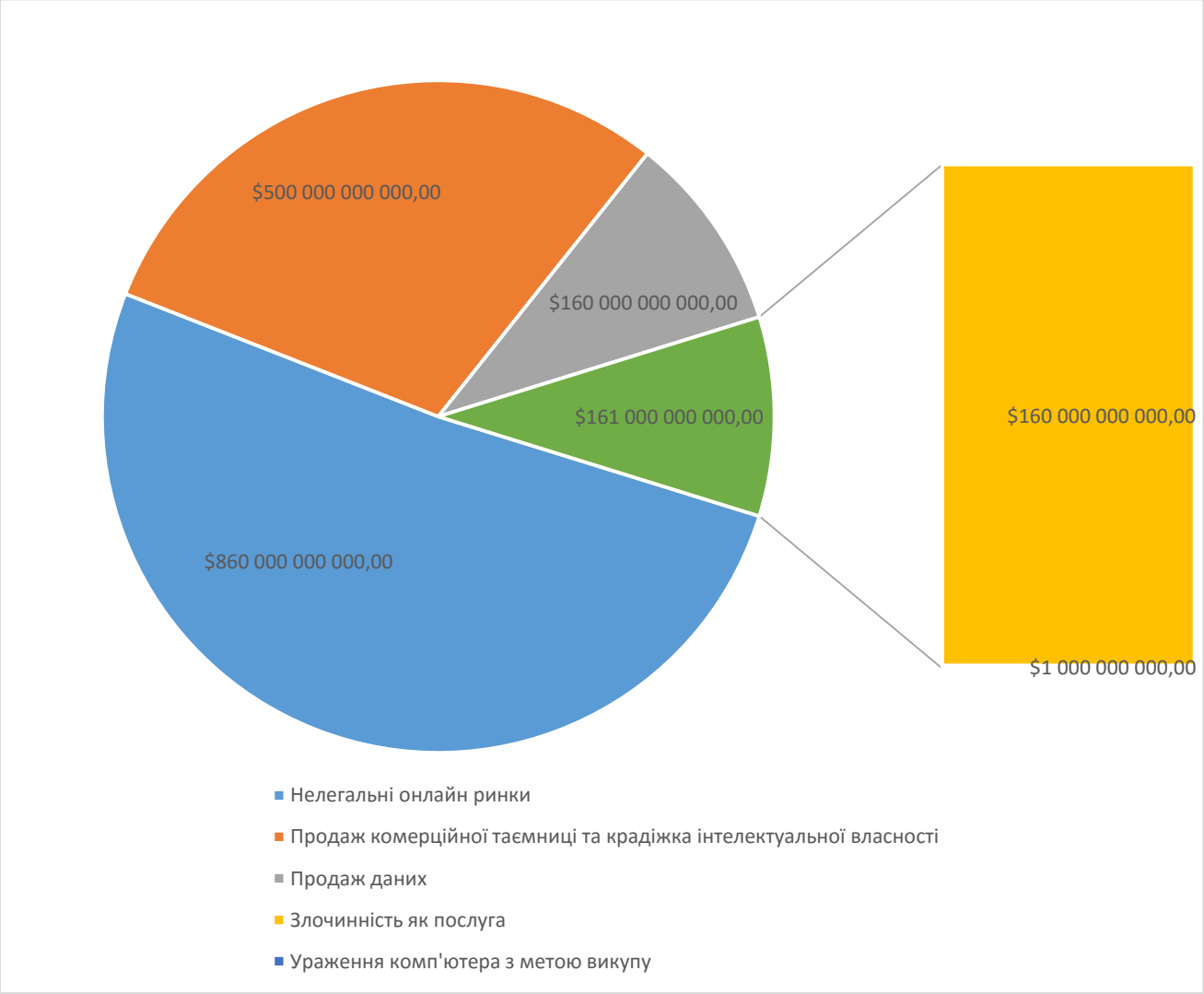
39. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : закон

України від 3 жовтні 2017 р. № 2147-VIII // Відомості Верховної Ради України. – 2017. – № 48. – Ст. 436.

40. 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.

Додаток

Доходи від кіберзлочинів (щорічні) *



* Дані наведено відповідно до: Re-Hashed: 2018 Cybercrime Statistics: A closer look at the “Web of Profit” Read more at: https://www.thesslstore.com/blog/2018-cybercrime-statistics/ [Електронний ресурс] // Hashedout. – 2018. – Режим доступу до ресурсу: https://www.thesslstore.com/blog/2018-cybercrime-statistics/

Анотація

В роботі досліджено становлення та розвиток міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю, встановлено зміст поняття та ознаки кіберзлочину в міжнародному праві, аргументовано наявність міжнародно-правового звичаю щодо змісту поняття кіберзлочину, наведено види та класифікацію кіберзлочинів, виявлено вплив змісту поняття кіберзлочину на характер міжнародного співробітництва держав у боротьбі з кіберзлочинністю, систематизовано ознаки кіберзлочинів. Також, досліджено та описано механізми міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю на універсальному та регіональному рівні, визначено спільні та відмінні риси такого співробітництва; проаналізовано проект конвенції з врегулювання такого співробітництва на універсальному рівні. Окрему увагу приділено стану імплементації Україною міжнародно-правових норм у сфері боротьби з кіберзлочинністю та виявлено потреби у вдосконаленні українського законодавства відповідно.

Актуальність теми: У XI столітті злочинність набула нових форм та все частіше злочини здійснюються шляхом використання мережі Інтернет. Виявлення загроз, розслідування таких діянь, а також притягнення винних осіб до відповідальності вимагає активного співробітництва державних органів, яке має мати швидкий характер та забезпечувати невідкладний доступ до даних, що часто знаходяться під юрисдикцією іншої держави. Як наслідок, діючі механізми міжнародно-правового співробітництва та допомоги є неефективними. Крім того, системи права багатьох держав повинні передбачати відповідні матеріальні та процесуальні норми, які, inter alia, повинні бути гармонізовані. Незважаючи на активне співробітництво держав у сфері боротьби з кіберзлочинністю через діяльність у міжнародних регіональних організацій, актуальним залишається питання створення універсального міжнародно-правового механізму, який забезпечить

холістичний підхід до імплементації державами стандартів, необхідних для полегшення такого співробітництва.

Мета і завдання дослідження. *Метою роботи* є аналіз міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю та імплементації Україною міжнародно-правових норм у цій сфері.

Досягнення зазначеної мети зумовило необхідність вирішення таких завдань: дослідити генезис міжнародно-правового регулювання боротьби з кіберзлочинністю; проаналізувати поняття та ознаки кіберзлочину у міжнародному праві; виявити міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні; визначити міжнародно-правовий механізм боротьби з кіберзлочинністю на регіональному рівні; проаналізувати ступінь імплементації Україною міжнародно-правових норм у сфері боротьби з кіберзлочинністю, виявити потреби у вдосконаленні відповідного законодавства.

Об'єкт дослідження. Об'єктом дослідження є міжнародні правовідносини у сфері боротьби з кіберзлочинністю.

*Предмет дослідження***.** Предметом дослідження є міжнародно-правове співробітництво держав у боротьбі з кіберзлочинністю.

Методи дослідження*:* Під час дослідження було використано загальні та спеціальні методи. Загальними методами наукового пізнання, що було застосовано, є індукція, за допомогою якої зроблено висновок про наявність та характер міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю, формально-логічний метод, який дав змогу класифікувати види кіберзлочинів у міжнародному праві, та аналіз, з використанням якого було встановлено характер міжнародно-правового співробітництва держав у боротьбі з кіберзлочинності шляхом їх участі в регіональних конвенціях та діяльності в регіональних міжурядових організаціях. Також, у роботі використано спеціально-юридичні методи дослідження: становлення та розвиток міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю було досліджено за допомогою історико-правового методу,

порівняння положень регіональних конвенцій про кіберзлочинність, а також рішень міжнародних організацій – порівняльно-правового, встановлення змісту міжнародно-правового звичаю щодо поняття кіберзлочину – формально-юридичного методу пізнання.