МІЖНАРОДНО-ПРАВОВІ ЗАСАДИ СПІВРОБІТНИЦТВА У БОРОТЬБІ З КІБЕРЗЛОЧИНАМИ

АНУФРІЄВ Микола Іванович - доктор юридичних наук, доцент МОН Навчально-науковий Інститут права ім. князя Володимира Великого МАУП-м. Київ

КІСІЛЕВИЧ-ЧОРНОЙВАН Ольга Михайлівна - доктор філософії права, Навчально-науковий Інститут права ім. князя Володимира Великого МАУП

УДК:341(045): 004.056

В данной научной статье исследуется международно-правовая система норм, направленных на создание правовых основ сотрудничества государств в сфере борьбы с киберпреступностью. Автор анализирует главные международные документы в данной сфере и определяет пути совершенствования ее правового регулирования.

Ключевые слова: киберпреступпреступление, международно-правовое регулирование, сотрудничество государств в борьбе с преступностью.

Прискорення розвитку інформаційного суспільства приносить країнам великі переваги в багатьох сферах суспільного життя. Однак створення нових можливостей для подальшого розвитку й використання інформаційних технологій неминуче тягне за собою виникнення відповідних проблем в інформаційній сфері. Однією з таких проблем, яка в останні роки набуває все більш глобального масштабу, є вчинення злочинів у сфері інформаційно-комунікаційних технологій (ІКТ). Дане явище посилюється не тільки в локальному, а і в світовому масштабі, що несе вже загрозу всій системі міжнародної інформаційної безпеки.

Поява таких комп'ютерних злочинів, що мають транснаціональний характер, їх кількість, латентність і складність зробили цілком зрозумілим висновок про те, що жодна з держав не зможе боротися з ними, покладаючись виключно на власні сили. Як наслідок, з'явилась потреба у міжнародному співробітництві [1, с.1].

Зважаючи на актуальність даної проблематики, на сьогодні існує велика кількість наукових і науково-практичних розробок, присвячених даному питанню. Серед них можна виділити праці І. Бачило, О. Баранова, А. Ю. Батурина, П. Біленчука, А. Жодзішського, І. Забари, Д. Біго, М. Герке, М. Дюмонтьє, А. Венгерова, В. Карпенко, Б. Кормича, В. Ліпкана, В. Лопатіна., І. Маланича, В. Талімончик, Х. Толеубекова тощо.

Метою даної наукової статті є системне дослідження міжнародно-правової системи співпраці у боротьбі з кіберзлочинами.

Досягнення поставленої мети зумовило необхідність розв'язання таких завдань:

· систематизувати і консолідовано представити міжнародно-правові документи у сфері співпраці у боротьбі з кіберзлочинами;

· визначити глибину впливів міжнародно-нормативних актів на вирішення вказаної проблеми шляхом компаративного аналізу та оцінки чинних міжнародних документів;

· розкрити ключові положення основних міжнародно-правових документів у сфері співпраці держав з протидії кіберзлочинам.

Враховуючи актуальність даного питання, багато міжнародних організацій (ООН, ЄС, РЄ, МСЕ, ШОС, ОЕСР тощо) включили в напрями своєї діяльності розробку нор-

мативної бази для сприяння співпраці у боротьбі з кіберзлочинами та створення органів, покликаних налагодити таку співпрацю.

Аналіз стратегій міжнародного співробітництва у сфері боротьби з кіберзлочинами на сучасному етапі свідчить як про спільні, так і про відмінні особливості концептуальних, доктринальних та прикладних підходів до міжнародної співпраці міжнародних організацій у даній сфері, що обумовлено різним баченням пріоритетів у сфері інформаційної безпеки держав-учасниць цих інституцій, пов'язаним, у свою чергу, з різним рівнем їх інформаційного розвитку.

Міжнародні документи прийняті в даній сфері умовно можна поділити на ті, що: 1) визнають існування проблеми і закликають до боротьби з цими злочинами; 2) закладають основи співробітництва у боротьбі з кіберзлочинами та /або надають визначення окремим видам злочинів міжнародного характеру у сфері ІКТ; 3) заснують органи, які покликані проводити заходи щодо боротьби з даними видами злочинів або створюють платформи для співробітництва в цій сфері (конференції, форуми тощо).

Потрібно відмітити, що на сьогодні ні в доктрині, ні в практиці не існує чіткого визначення поняття комп'ютерного злочину, дискутуються різні точки зору з питань їх класифікації. Складність у формулюванні цих понять існує як внаслідок неможливості виділення єдиного об'єкта злочинного посягання, так і множинністю предметів злочинного посягання з точки зору їх кримінально-правового значення [2]. Неоднозначність цього явища призвела до застосування таких термінів, як «комп'ютерні злочини», «високотехнологічні злочини», «злочини у сфері комп'ютерної інформації», «кіберзлочини», «інформаційні злочини» і т.д., у які вкладаються досить різні поняття. Це знайшло відображення і в міжнародно-правових актах.

Вищезгадана перша група міжнародних актів в основному представляє собою так зване «soft low». Серед них особливо можна відмітити резолюції ГА ООН, які або в цілому присвячені даному питанню (Резолюції ГА ООН "Боротьба зі злочинним використанням інформаційних технологій; № 55/63 від 4 грудня 2000 року, № 56/121 від 19 грудня 2001 року), або розглядають його в контексті інформаційної безпеки (Декларації тисячоліття ООН 2000 р., Резолюції ГА ООН «Досягнення у сфері інформації та комунікації в контексті міжнародної безпеки» № 53/70 від 4 грудня 1998 року, № 54/49 від 1 грудня 1999 року, № 55/28 від 20 листопада 2000 року, № 56/19 від 29 листопада 2001 року, № 57/53 від 22 листопада 2002 року, № 58/32 від 8 грудня 2003 року, № 59/61 від 3 грудня 2004 року, № 60/45 від 8 грудня 2005 року, № 61/54 від 6 грудня 2006 року, № 62/17 від 5 грудня 2007 року, № 63/37 від 2 грудня 2008 року, № 64/25 від 2 грудня 2009 року, № 65/41 від 8 грудня 2010 року, № 66/24 від 13 грудня 2011 року, Резолюція ГА ООН 56/27 "Заходи з ліквідації міжнародного тероризму" 2003 р., Резолюції ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» №57/239 від 20 грудня 2002 року, № 58/199 від 23 грудня 2003 року, № 64/211 від 21 грудня 2009 року, Декларація принципів «Побудова Інформаційного суспільства — глобальне завдання в новому тисячолітті» 2003 р. тощо). Крім того, Економічна і Соціальна Рада ООН прийняла Резолюції «Міжнародне співробітництво у справі щодо попередження і розслідування шахрайства, злочинного неправомірного використання і фальсифікації особистих даних і пов'язаних з ними злочинів, а також переслідування та покарання за них» № 2004/26 від 21 липня 2004 року,- № 2007/20 від 26 липня 2007 року.

Велику увагу боротьбі з кіберзлочинами приділяє і Міжнародний союз електрозв'язку. До актів організації, які визнають існування проблеми кіберзлочинів і закликають до боротьби з ними, відносять Резолюцію 71 (переглян. 2014 р.) «Стратегічний план Союзу на 2016 – 2019 років», Резолюцію 130 (переглян. 2014 р.) «Посилення ролі МСЕ в зміцненні довіри і безпеки при використанні інформаційно-комунікаційних технологій», Резолюцію 174 (переглян. 2014 р.) «Роль МСЕ у зв'язку з питаннями міжнародної державної політики, що стосуються ризику незаконного використання

інформаційно-комунікаційних технологій», Резолюцію 181 (Гвадалахара 2010 р.) «Визначення і термінологія, пов'язані зі зміцненням довіри і безпеки при використанні інформаційно-комунікаційних технологій» тощо [4].

Діяльність ОЕСР у галузі боротьби з кіберзлочинами в основному спрямовується на проведення досліджень, пов'язаних із можливістю гармонізації кримінального законодавства в даній сфері. У 1992 році Радою ОЕСР було прийнято «Керівні принципи з інформаційної безпеки». Цей документ передбачає прийняття країнами національних положень для забезпечення цілісності і конфіденційності інформаційних систем та інформації, яка в них обробляється, через прийняття комплексу організаційних і технічних захисних заходів. У 2002 році нова версія принципів «Керівні принципи ОЕСР із забезпечення безпеки інформаційних систем і мереж: до культури безпеки» була рекомендована Радою ОЕСР. Дані документи є мінімальними стандартами, які створені в результаті консенсусу між позиціями країнчленів ОЭСР.

У ЄС проблема кібербезпеки в першу чергу зосереджена на захисті цілісності інформації та інформаційної системи, гарантуванні належних умов її обігу та цінності. Серед нормативних актів у даній сфері можна виділити Резолюцію про стратегію інформаційного суспільства в Європі 2007 р. (Résolution du Conseil du 22 mars 2007 relative á un stratégie pour une société de l'information sûre en Europe), Рішення про багаторічний план дій Співтовариства зі сприяння безпечному використанню Інтернету шляхом боротьби із незаконним і шкідливим змістом у глобальних мережах № 276/1999/ЄС від 25 січня 1999 р. (Програма «Безпечний Інтернет» (1999–2004 рр.), «Безпечний Інтернет Плюс» (2005–2008 рр.), «Безпечний Інтернет 2009–2013 рр.», Спільне повідомлення для Європейського Парламенту, Європейської Ради, Європейського економічно-соціального комітету та Комітету регіонів «Перегляд Європейської політики сусідства» 2015 р. [5]. «План дій «Безпечний Інтернет» (1999-2004 рр.)» був покликаний сприяти формуванню сприятливого середовища для розвитку Інтернету в межах ЄС, прийняття кодексу поведінки глобальних мереж та можливої гармонізації правової термінології. Крім того, у межах ЄС було прийнято низку програм для вирішення проблем кіберзлочинності, зокрема такі: «Електронна Європа», «План дій щодо Інтернету», «Технології інформаційного суспільства». Програми ЄС «Попередження й боротьба зі злочинністю» передбачали ключові моменти співробітництва у сфері протидії кіберзлочинності [3, с. 177].

Важливим внеском ШОС у справі створення основ міжнародного співробітництва став документ, який було винесено на обговорення під час 66-ї сесії Генеральної Асамблеї ООН під назвою «Конвенція про забезпечення міжнародної інформаційної безпеки». Основною метою цього документу було визначення прав та обов'язків держав в інформаційному просторі, стимулювання їх відповідальної поведінки та посилення співробітництва, в тому числі в боротьбі з комп'ютерними злочинами. Акт так і не прийняли.

Усі вищевказані документи, хоча у своїй більшості і носять рекомендаційний характер, однак створюють підґрунтя для подальшої співпраці держав у розв'язанні теоретичних та практичних питань у даній сфері на глобальному та регіональному рівнях.

На даний момент актів другого типу існує небагато, оскільки визнати певні злочини як злочини міжнародного характеру (міжнародні кримінальні злочини) та реалізувати на практиці повноцінне багатостороннє співробітництво у боротьбі з ними досить важко завдяки багатьом факторам.

Міжнародні акти в цій сфері до міжнародних кримінальних злочинів відносять різні категорії правопорушень, або виписують їх по-різному. Так у Конвенції РЄ «Про кіберзлочинність» 2001 р. та Додатковому протоколі до неї 2003 р. до злочинів міжнародного характеру відносять: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до цілої комп'ютерної системи або її частини; нелегальне перехоплення технічними засобами передач комп'ютерних даних; втручання

у дані; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних; зловживання пристроями); 2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами); 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією, правопорушення, пов'язані з расистським та ксенофобним матеріалом); 4) правопорушення, пов'язані з порушенням авторських та суміжних прав. Конвенція встановлює також відповідальність за спробу, допомогу чи співучасть і корпоративну відповідальність [6]. Тобто в поняття «кіберзлочин» включається декілька різнопланових протиправних посягань.

Угода СНД «Про співпрацю держав-учасниць СНД у боротьбі із злочинами у сфері комп'ютерної інформації» дає трохи інший і вужчий перелік злочинів у даній сфері, який відповідає злочинам, що визначені Конвенцією РЄ як правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем та правопорушення, пов'язані з комп'ютерами, не включаючи правопорушення, пов'язані зі змістом (у сенсі конвенції РЄ), та трактуючи правопорушення пов'язані з порушенням авторських та суміжних прав, як незаконне використання програм для ЕОМ і баз даних, які є об'єктами авторського права та/чи присвоєння авторства [7].

Угода між урядами держав-членів Шанхайської організації співпраці «Про співпрацю в області забезпечення міжнародної інформаційної безпеки 2009 р.» у додатку 1 взагалі дає тільки визначення «інформаційної злочинності» (як використання інформаційних ресурсів і (чи) дія на них в інформаційному просторі в протиправних цілях) [8].

У Повідомленні від Комісії Раді ЄС, Європарламенту, Економко-соціальному комітету та комітету регіонів «Створюючи безпечніше інформаційне суспільство через покращення безпеки інформаційних інфраструктур і борючись із комп'ютерними злочинами» 2002 р., відмічається, що існують різні погляди на те, що ж складає «комп'ютерний злочин». Відмінність може бути визначена між комп'ютерними специфічними злочинами та традиційними злочинами вчиненими за допомогою комп'ютерних технологій. Відносно комп'ютерних специфічних злочинів у ЄС існує ряд прямих і не прямих відповідних законних інструментів : порушення приватності — Директива 95/46/ЄС Європейського Парламенту та Ради від 24 жовтня 1995 року про захист індивідуумів щодо обробки персональних даних та вільної передачі таких даних та Директива 97/66/ЄС від 15 Грудня 1997 року про обробку персональних даних та забезпечення приватності в телекомунікаційному секторі; порушення пов'язані зі змістом — Рішення Ради від 29 Травня 2000 року про боротьбу з дитячою порнографією в Інтернеті; економічні злочини, несанкціонований доступ та диверсії — Рамкове рішення ЄС «Про атаки на інформаційні системи» 2005 р.; злочини у сфері інтелектуальної власності — Директива Ради 91/250/ЄЕС від 14 травня 1991 року про правовий захист комп'ютерних програм (OB L 122, 17.05.1991, C. 42-46), Директива 96/9/ЄС Європейського Парламенту та Ради від 11 березня 1996 року про правовий захист баз даних [4].

Рамкове рішення ЄС «Про атаки на інформаційні системи» 2005 р. передбачає відповідальність за три категорії навмисних злочинів : 1) незаконний доступ до інформаційних систем; 2) посягання на недоторканість системи; 3) посягання на недоторканість даних. На відміну від вищевказаних нормативних актів, які покладають обов'язок самим визначити кримінально-правові санкції, Рамкове рішення зобов'язує держав-членів встановити конкретні строки тюремного ув'язнення за дві останні категорії злочинів [9, с. 964].

Міжнародними документами встановлено різні форми та глибину співпраці. Наприклад, «Глобальна програма кібербезпеки» МСЕ 2007 р. і серед форм співпраці визначає розробку глобальних стратегій у сфері створення відповідного типового законодавства у сфері боротьби з комп'ютерною злочинністю, національних та регіональних організаційних структур, створення глобальної

структури для спостереження, сповіщення і реагування на інциденти тощо, підготовку відповідних пропозицій, співпрацю на рівні регіональних та глобальних конференцій [4].

Найбільша кількість форм співробітництва прописана в Конвенції СНД. Однак, найбільш докладніше процедура співпраці по формах співробітництва виписана в Конвенції РЄ. Крім того, дана Конвенція встановлює юрисдикцію країн-членів стосовно будь-якого злочину, встановленого відповідно до статей конвенції (крім корпоративної відповідальності).

Питання, які не висвітлено в даних міжнародних нормативних актах вирішуються відповідно до конвенцій та угод про співпрацю у сфері правової допомоги та національного законодавства.

Відповідно до вищевказаної третьої групи міжнародних актів було створено органи та платформи для співпраці, які мають різні повноваження і цілі : від обговорення проблем кіберзлочинності до реальних дій у боротьбі з кіберзлочинами. Серед них варто назвати : МСЕ — регіональні конференції та Група експертів високого рівня з питань кібербезпеки (HLEG) (відповідно до «Глобальної програми кібербезпеки» МСЕ 2007 р займається забезпеченням подальшої розробки Глобальної програми кібербезпеки, аналізом існуючих загроз для кібербезпеки, передбаченням виникаючих і майбутніх проблем, досягненням цілей Програми тощо); РЄ — Комітет експертів для обговорення питань кіберзлочинів (відповідно до Рішення CDPC/103/211196), Комітет експертів із злочинів у Кіберпросторі (відповідно до Рішення№ CM/Del/Dec(97)583); ЄС — Європейськое агентство з мережевої та інформаційної безпеки (відповідно до Регламенту Парламенту та Ради ЄС 2004 р.), Комп'ютерна група швидкого реагування (допомагає боротися з новітніми комп'ютерними вірусами, розробляє інтернет-стратегію для Єврокомісії), Європейський центр боротьбі з кіберзлочинністю (сформовано у 2014 р. відповідно до стратегії внутрішньої безпеки ЄС 2011 р.; займається інформаційною, оперативною та експертною підтримкою розслідуванням на міжнародному та регіональному рівнях); у 2006 р. заснована Міжнародна організація по боротьбі з кібертероризмом «ІМПАКТ» (об'єднала в собі представників державного і комерційного секторів для пошуку і реалізації найбільш ефективних шляхів протистояння кібертероризму).

Підбиваючи підсумки, потрібно відмітити, що проблемам боротьби з кіберзлочинами приділяє увагу багато міжнародних організацій, однак у більшості випадків вона зосереджується на концептуальних дослідженнях даної проблематики в контексті інформаційної безпеки. При цьому ООН та його спеціалізовані установи виступають найбільшими платформами для обговорення питання боротьби з кіберзлочинами.

Співробітництво держав відносно криміналізації певних видів кіберзлочинів та боротьби з ними, включаючи створення відповідних органів, в основному розвивається в рамках міжнародних регіональних організацій.

Крім того, регіональними міжнародними актами прописано різні форми та глибина співпраці, покладаючи вирішення багатьох процедурних питань на угоди між країнами про співпрацю у кримінальних справах.

І на кінець, сьогодні вже існує необхідність у вироблені міжнародної конвенції, яка б на глобальному рівні криміналізувала кіберзлочини (на кшталт конвенцій РЄ та СНД), визначила форми співпраці (можливо, більш глибокі за існуючі на даний час) між країнами у боротьбі з такими злочинами, створила інституційний механізм по боротьбі з кіберзлочинами, що відповідав би потребам сьогодення, та закріпила юрисдикцію країн-членів у даній сфері.

Література

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

2. Голубєв В.О. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій [Текст]: навч. посіб./ В.О. Голубєв, В.Д. Гавловський, В.С. Цимбалюк та ін.; за ред. д.ю.н., професора Р.Н. Калюж-

АНОТАЦІЯ

В даній науковій статті досліджується міжнародно-правова система норм, спрямованих на створення правових засад співробітництва держав у сфері боротьби з кіберзлочинами. Автор аналізує головні міжнародні документи в даній сфері та визначає шляхи удосконалення її правового регулювання.

Ключові слова: кіберзлочин, міжнародно-правове регулювання, співробітництво держав у боротьбі зі злочинністю.

ного.— Запоріжжя: ГУ «ЗІДМУ», 2002. — 292 с.

3. Грицун О.О. Регулювання питань міжнародної інформаційної безпеки в межах міжнародних організацій/ О.О. Грицун // Вісник Запорізького національного університету.— № 4 (І).— 2014.— 172-180.

4. http://www.itu.int/ru/Pages/default.aspx.

5. http://europa.eu/european-union/index_fr.

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

SUMMARY

In this scientific article the system of international legal norms aimed at creating legal bases of cooperation of states in the field of cybercrime. The author analyzes the main international instruments in this field and determine ways to improve its regulation.

Tags: cybercrime, international legal regulation, cooperation of States in combating crime.

7. Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації від 1 червня 2001 року [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/997_353.

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

9. Право Европейского союза : учебник для вузов / под ред. С.Ю. *Кашкина*. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт; Высшее образование. 2010 — 1119 с.