СЕКЦІЯ 5.
Правові основи господарської діяльності та фінансово-економічної безпеки

SECTION 5.
The legal framework of economic activities, financial and economic security

Арндт К.
студентка III курсу
факультету міжнародних відносин
Східноєвропейського національного університету
ім. Лесі Українки
Науковий керівник: к.політ.н.,
доцент кафедри міжнародних відносин
і регіональних студій СНУ
Вознюк Є.В.

МІЖНАРОДНА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ

За останні два десятиліття тема кіберзлочинності стала не лише звичною в заголовках новин, а й однією з найбільш обговорюваних у рамках експертних спільнот та міжнародних організацій. Хоча ООН відносить кіберзлочини до «нових злочинів», наголошується, що це явище має глобальний характер та містить елементи транснаціональності, що робить міжнародне співробітництво ключовим фактором прийняття ефективних заходів протидії.

Загальновизнаним транснаціональний характер кіберзлочинності поряд із децентралізованою структурою є одними з базових проблем боротьби зі злочинністю в кіберпросторі: по-перше, відсутні механізми контролю, необхідні для правозастосування, по-друге, існують серйозні труднощі для розслідування злочинів і визначення юрисдикції. Традиційні підходи до боротьби зі злочинністю, засновані на територіальному принципі визначення юрисдикції, виявляються неефективними. Кіберпростір по суті своїй є міжнародним. Потрібне активне міжнародно-правове співробітництво, гармонізація матеріальних і процесуальних норм права, пошук нових підходів до міжнародної співпраці.

Більшість провідних міжнародних організацій, діяльність яких пов'язана із забезпеченням безпеки у світі, захистом прав людини, захистом інформації, протягом останнього десятиліття вживають активних зусиль для налагодження міжнародного співробітництва в цій галузі. Активну роль відіграє Організація Об'єднаних Націй.

У 2010 році підсумком 12-го Конгресу щодо запобігання злочинності та кримінального правосуддя стало створення міжурядової групи експертів відкритого складу для дослідження проблеми кіберзлочинності і заходів у відповідь з боку країн-членів, міжнародної спільноти та приватного сектора [1]. Управління Організації Об'єднаних Націй із наркотиків і злочинності у 2013 році підготувало Всебічне дослідження проблеми кіберзлочинності. Згідно з висновками експертів, більшість держав світу не вважають за необхідне появу додаткових форм юрисдикції щодо «кіберпростору», оскільки успішне міжнародне співробітництво можливе в рамках наявних механізмів. Однак самі експерти відзначають, що наявні повноваження і процедури співробітництва часто не враховують «особливості електронних доказів і глобальний характер кіберзлочинності». Приклади ефективної кооперації засновані на правовій співпраці деяких держав, які за допомогою регіональних угод створюють необхідний рівень гармонізації своїх правових норм і правові механізми взаємодії з урахуванням специфіки кіберзлочинів, зокрема, через Конвенцію Ради Європи про кіберзлочинність і Конвенцію Ліги арабських держав про боротьбу зі злочинами в області інформаційних технологій.

Таким чином спостерігається тенденція до фрагментації міжнародно-правового співробітництва, що відображає внутрішній парадокс розвитку міжнародних відносин у цифрову епоху: з одного боку, країнам необхідна співпраця в боротьбі з транснаціональними загрозами, з іншого боку, ця співпраця веде до зростання потенційної уразливості кожної держави, вимушеного обмежувати свій суверенітет у двох чутливих областях – кримінальному праві та захисті інформації. Внаслідок цього успішна співпраця реалізується в регіонах, де є досить високий рівень політичної довіри між учасниками, зокрема в Європі.

Першим етапом стало прийняття Радою Європи Конвенції з кіберзлочинності у 2001 році [2], положення якої сприяли гармонізації норм основних комп'ютерних злочинів та заклали основи процесуальної співпраці правоохоронних органів країн-учасниць Конвенції. Успіх Конвенції в тому, що сфера її дії вийшла за межі європейського регіону: її підписали і ратифікували Аргентина, Австралія, Ізраїль, Японія, США та інші країни. Таким чином, Конвенція 2001 року продовжує залишатися досить успішним, але регіональним інструментом співпраці.

Надалі країни-члени Європейського союзу максимально поглибили співпрацю в області кібербезпеки через інструменти європейського права. Норми матеріального права гармонізовані за допомогою цілого ряду директив, зокрема, Директива про протидію сексуальних експлуатації дітей онлайн і дитячої порнографії, Директива щодо атак проти інформаційних систем, Директива про безпеку мереж та інформаційних систем. Створено загальноєвропейські агентства для організації співпраці правоохоронних органів, судових органів, відомств, що відповідають за інформаційну та мережеву безпеку.

Фундаментом для позитивного зрушення в цій галузі є розуміння, що повноцінна боротьба з кіберзлочинністю неможлива без комплексної міжнародної взаємодії. Для переходу на наступний етап і гармонізації кримінального законодавства необхідно досягти загального розуміння кримінальних загроз у кіберпросторі [3].

Для аналізу загроз, моніторингу ситуації, експертної перевірки, формування інформаційного пулу необхідно створення спеціальних відомств або підрозділів на міжнародному рівні з чітким мандатом діяльності і чіткими правилами співпраці з компетентними органами різних держав. Необхідне розширення діяльності Європейської робочої групи Інтерполу з комп'ютерної злочинності.

Особливістю кіберзлочинів крім їх транснаціонального характеру є той факт, що комплексна боротьба з ними можливо із залученням не різних держав світу, а й недержавних акторів, включаючи приватні компанії та окремих осіб – учасників інформаційної взаємодії. Адже не тільки держави, а й кожна людина стає уразливою. У зв'язку з цим важливим завданням є підвищення інформованості населення.

Стан міжнародного співробітництва у сфері боротьби з кіберзлочинністю на сьогодні не є однозначним. Вона впливає не тільки на розвинені країни: Інтернет-користувачі є по всьому світу, державні установи в країнах, що розвиваються активно використовують інформаційні технології. Зрозуміло, що для ефективної боротьби з кіберзлочинністю потрібне глобальне співробітництво. Також потрібна розробка універсального документа. Для реалізації цього завдання слід використовувати наявний регіональний досвід та дійти консенсусу з питань визначення основних понять та критичних загроз.

Список використаних джерел

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

2. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. [Електронний ресурс]. – Режим доступу: //www.zakon2.rada.gov.ua/laws/show/994_575.

3. Всестороннее исследование проблемы киберпреступности [Електронний ресурс]. – Режим доступу: https://www.unodc.org/documents/organized–crime/cybercrime/Cybercrime_Study_Russian.pdf.