УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор*,
директор Навчально-наукового інституту перепідготовки та підвищення кваліфікації кадрів СБУ Національної академії Служби безпеки України

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У БОРОТЬБІ З ТРАНСНАЦІОНАЛЬНОЮ КІБЕРЗЛОЧИННІСТЮ

Анотація. *У статті досліджуються питання міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю. Сформульовано пропозиції щодо покращення співробітництва вітчизняних правоохоронних органів із зарубіжними партнерами з метою підвищення оперативності розслідування відповідних злочинів.*

Ключові слова*: міжнародне співробітництво, кіберзлочин, правоохоронні органи, транснаціональна кіберзлочинність.*

Summary. *The article deals with the issues of international cooperation in counteraction to transnational cybercrimes. The proposals on improvement of cooperation between domestic law enforcement agencies and foreign partners are formulated in order to increase the efficiency of the investigation of cybercrime.*

Keywords: *international cooperation, cybercrime, law enforcement agencies, transnational cybercrimes.*

Аннотация. *В статье исследуются вопросы международного сотрудничества в борьбе с транснациональной киберпреступностью. Сформулированы предложения по усовершенствованию сотрудничества отечественных правоохранительных органов с иностранными партнерами с целью повышения оперативности расследования соответствующих преступлений.*

Ключевые слова. *Международное сотрудничество, киберпреступление, правоохранительные органы, транснациональная киберпреступность.*

Постановка проблеми. Міжнародне право має численні джерела, які прямо або опосередковано регламентують співробітництво правоохоронних органів у боротьбі з транснаціональною кіберзлочинністю. Основним таким документом безумовно є Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. (далі – Конвенція), яка спрямована на підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, на надання можливості збирання електронних доказів тощо [1]. Зазначена Конвенція має не регіональний, а фактично міжнародний характер.

Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21 грудня 2010 р. та Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16 червня 2009 р. мають регіональний характер і також спрямовані на боротьбу з транснаціональною кіберзлочинністю.

Однак міжнародна спільнота намагається сформувати додаткові правові і організаційні передумови для підвищення ефективності протидії транснаціональній кіберзлочинності. Наприклад, у лютому 2016 року ЄС та НАТО підписали технічну угоду щодо посилення співпраці у сфері кібербезпеки, спрямованої на створення сприятливих умов задля оперативного обміну інформацією та досвідом між командами екстреного реагування НАТО “Computer Incident Response Capability” (NCIRC) та ЄС

“Computer Emergency Response Team of the European Union” (CERT-EU) у сфері протидії кібератакам, комплексного протистояння сучасним викликам у кіберпросторі.

Для України особливої актуальності набуває досвід міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю, насамперед приклади результативної взаємодії правоохоронних органів у цій сфері.

Результати аналізу наукових публікацій свідчать про те, що питання співробітництва іноземних держав та їх правоохоронних органів у боротьбі з транснаціональною кіберзлочинністю були предметом досліджень лише частково. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як О. Бойченко, В. Брижко, В. Бутузов, А. Войціховський, В. Марков, В. Пилипчук, К. Тітуніна, М. Швець, О. Юрченко та інші. Автор розпочав розгляд дотичних питань у контексті проблем розслідування кіберзлочинів в Україні [2].

Метою статті є розкриття досвіду міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю задля визначення можливостей його використання в Україні.

Виклад основного матеріалу. На сучасному етапі правоохоронні органи іноземних держав взаємодіють у межах розслідування транснаціональних кіберзлочинів переважно на підставах, передбачених ст.ст. 24 – 35 Конвенції у таких напрямках як: екстрадиція; взаємна допомога (як з метою розслідування злочинів, пов’язаних з комп’ютерними системами та даними, так і з метою збирання доказів у електронній формі щодо кримінального правопорушення); добровільна допомога (правоохоронний орган у межах національного законодавства без попереднього запиту надсилає іноземному партнеру інформацію, отриману в ході його розслідування, якщо вважає, що розкриття такої інформації може допомогти партнеру у відкритті або проведенні розслідування кіберзлочинів); взаємна допомога щодо тимчасових заходів, яка включає термінове збереження комп’ютерних даних, які зберігаються; термінове розкриття збережених даних про рух інформації; взаємна допомога щодо доступу до комп’ютерних даних, які зберігаються; транскордонний доступ до комп’ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними; взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу; взаємна допомога у перехопленні даних змісту інформації; цілодобова мережа для обміну інформацією [1].

Важливе значення для співробітництва між державами у сфері боротьби з транснаціональною кіберзлочинністю мають двосторонні та багатосторонні міжнародні договори про взаємну правову допомогу, взаємне визнання іноземних судових рішень, адже на їх основі також відбувається співпраця між правоохоронними органами різних країн.

На сьогодні існує потреба прийняття на рівні ООН універсального міжнародно-правового акту, наприклад, Конвенції протидії кіберзлочинності. Окремі організаційні передумови для цього є. Так, Глобальна програма з кіберзлочинності, відповідно до резолюції Генеральної Асамблеї 65/230 і Комісії з попередження злочинності та кримінального правосуддя резолюції 22/7 і 22/8, передбачає допомогу державам-членам у їх боротьбі з кіберзлочинами, пов’язану переважно з технічною допомогою, яка фінансується за рахунок підтримки урядів Австралії, Канади, Японії, Норвегії, Великобританії і США [3]. Корисними для вітчизняних правоохоронців є ресурси репозиторію ″Cybercrime″, створеного у 2015 році в межах Комісії з попередження злочинності і кримінального правосуддя, який містить бази даних законодавства,

прецедентного права (понад 180 країн) про кіберзлочинність та електронні докази, судову практику, а також записи успішних правоохоронних операцій щодо кіберзлочинів та збирання електронних доказів [4].

Найрезультативнішим є співробітництво правоохоронних органів різних країн у межах Інтерполу, оскільки ця організація має унікальний статус, який передбачає поглиблення боротьби з кіберзлочинністю у глобальному масштабі шляхом активного вивчення нових злочинів, новітніх методів навчання та розробки інноваційних інструментів поліцейської діяльності. Інтерпол через свої Національні центральні бюро в 190 країнах здійснює координаційні зусилля, в першу чергу через підтримку національної поліції, полегшення обміну інформацією та надання оновлень щодо розслідувань [5].

Показовою є операція з протидії кіберзлочинам під проводом Інтерполу у взаємодії з Асоціацією держав Південно-Східної Азії (АСЕАН), яка призвела до виявлення майже 9000 серверів команд і керування та сотень зловмисних веб-сайтів, включаючи державні портали. Операція об’єднала слідчих з Індонезії, Малайзії, М’янми, Філіппін, Сінгапуру, Таїланду, В’єтнаму та Китаю, а також експертів з компаній приватного сектору: Trend Micro, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet та Palo Alto Networks та інших. Було виявлено близько 270 сайтів, заражених шкідливим кодом, які використовували вразливість у застосуванні дизайну веб-сайту. Серед них було кілька державних веб-сайтів, які могли містити персональні дані громадян, виявлено декілька операторів фішингу, зловмисне програмне забезпечення, зокрема спрямоване на фінансові установи, на DDoS-атаки та розповсюдження спаму. Операція допомогла учасникам виявити та розслідувати різні види кіберзлочинів, які раніше не розслідувались у країнах-учасниках операції, сприяла навчанню обробки реальної кіберінформації, наданої приватними компаніями та Інтерполом [6].

Правозахисне агентство ЄС, Європол, а також його Об’єднана робоча група з боротьби з кіберзлочинністю, яка також включає в себе представників ФБР та спецслужб США, співпрацюють разом у розслідуванні кібератак [7]. Так, міжнародна операція, спрямована на шахраїв з авіаквитками, призвела до затримання 153 осіб, підозрюваних у використанні квитків, придбаних за краденими, підробленими кредитними картками. Операція відбувалася з 6 по 8 червня 2017 року за участі 64 країн, 84 авіакомпаній та 8 онлайнових туристичних агентств, які співпрацювали з працівниками правоохоронних органів для здійснення оперативних заходів у 230 аеропортах світу. Всього було повідомлено про 312 підозрілих операцій. Представники авіакомпаній, он-лайнові туристичні агентства, компанії з обслуговування платіжних карток, платформа для огляду міжнародної туристичної індустрії Perseuss та Міжнародна асоціація повітряного транспорту (IATA) надавали додаткову інформацію про підозрілі транзакції під час операції. Операція була скоординована з операційних центрів у Європі в Нідерландах, глобальному комплексі інновацій Інтерполу в Сінгапурі та Америполом в Боготі. Її також підтримали UNODC (AIRCOP для Африки), канадські та американські правоохоронні органи. Шахрайські онлайн-покупки авіаквитків призводять до збитків авіакомпанії до 1 млрд. дол. США на рік, є прибутковими для організованої транснаціональної злочинності і часто сприяють більш серйозній злочинній діяльності, включаючи нелегальну імміграцію, торгівлю людьми, контрабанду наркотиків та тероризм [8].

Поліція використовує за допомогою фахівців приватного сектору нові методики виявлення та припинення діяльності транснаціональної кіберзлочинності. Так, у межах операції Avalanche здійснювалось “просіювання” шкідливого Інтернет-трафіку. Коли,

наприклад, заражений комп’ютер намагається зв’язатися з його контролером, поліція за допомогою спеціальної технології фіксує це повідомлення та перешкоджає його зв’язку із фактичним центральним контролером. Таким чином, заражений комп’ютер не може передавати протиправні команди. Однак переривання технологічних систем недостатньо для того, щоб поліція зупинила злочинців. Починаючи з 2010 року тричі поліція намагалася зняти ботнет Kelihos. Операція Avalanche призвела до арешту п’яти осіб, які були керівниками організації. Їх усунення від злочинних дій, призвело до тимчасового “збою” в глобальному середовищі кіберзлочинності [9]. До речі, Департаментом кіберполіції Національної поліції України у межах спецоперації Avalanche здійснювались заходи щодо затримання на території України одного з основних фігурантів зазначеного провадження [10].

Активно використовуються іноземними державами технологічні рішення для боротьби з транснаціональною кіберзлочинністю. Так, Європол представив членам ЄС систему IOCTA (Internet Facilitated Organised Crime Tread Assessment), яка сприяє розкриттю кіберзлочинів. На даний час Європол надає членам ЄС слідчу і аналітичну підтримку через свою систему онлайн-розслідувань і базу даних злочинів [11].

Показовим є наступний приклад трансатлантичної співпраці. Так, два провідні он-лайн-анонімні ринки – Alpha Bay і Hansa Market – були заблоковані Федеральним бюро розслідувань (ФБР) та Голландським національним відділом злочинності високих технологій (NHTCU) під час операції “Байонет” [12]. ФБР вдалося порушити роботу AlphaBay – відомого даркнету, а NHTCU втрутився на даркнет-ринок Hansa протягом майже місяця як адміністратор, а потім закрив Hansa Market назавжди. Багато користувачів AlphaBay шукали притулок на ринку Hansa, на якому на той момент працювало NHTCU. Отже, поліцейські установи були в ідеальному становищі, щоб не тільки порушити екосистему, створюючи недовіру серед користувачів на цих анонімних ринках, а й збирати цінні дані на тисячі з них [13].

Набуває розвитку протиправна діяльність із використання криптовалют. Так, за статистикою кібервідділу Національного Агентства по боротьбі зі злочинністю Великої Британії (NCA) у 2013 році було зафіксовано вчинення кримінальних правопорушень із використанням криптовалюти на суму еквівалентну 3 млн. доларів США, у 2016 році – вже понад 100 млн. доларів США. Трендом у Британії стало використання злочинцями у протиправній діяльності сервісів з анонімізації криптовалютних транзакцій та повністю анонімних цифрових валют. Враховуючи те, що в Британії діє прецедентне право, фахівцям кібер-відділу NCA, розслідуючи злочин із використанням цифрової валюти, вдалось отримати позитивний судовий прецедент. Так, при розгляді справи в суді оперативниками було подано клопотання про вилучення і подальшу реалізацію біткоїнів, отриманих злочинним шляхом. У мотиваційній частині клопотання британськими спеціалістами було зазначено про те, що криптовалюта є різновидом майна, а отже до неї можливо застосувати загальне законодавство про збирання доказів та вилучення доходів, отриманих злочинним шляхом. У подальшому, тільки у 2017 році в Британії NCA було здійснено понад 10 успішних випадків вилучення криптовалюти у межах кримінальних проваджень [14].

Позитивним для України є той факт, що починаючи з 2019 року NCA нададуть доступ до спеціального програмного забезпечення, за допомогою якого можливо ефективно відслідковувати проведені криптовалютні транзакції у межах розслідування кримінальних злочинів, у повному обсязі підрозділам СБ України та Департаменту кіберполіції.

Заслуговують на увагу підходи іноземних держав щодо створення інституційних і технологічних передумов для протидії транснаціональній кіберзлочинності. Так, у Казахстані передбачено створення глобальної системи інформаційної безпеки “Кіберщит”, яка буде захищати від кібератак державні інформаційні ресурси.

У Китаї вступив в силу Закон про кібербезпеку КНР, прийнятий у жовтні 2016 року. У ньому передбачені загальні принципи і заходи мережевої безпеки, зокрема нагляд, заходи попередження і реагування у випадках кібератак. Крім того, стандартизація і державний контроль є основою безпеки Інтернету в Китаї, що дає правові можливості на законних підставах виявляти і документувати транснаціональні кіберзлочини.

Стратегія кібербезпеки Європейського Союзу [16] передбачає здійснення кіберзахисту за такими напрямами:

- виявлення і блокування кібератак, локалізації їх наслідків незалежно від походження стосовно об’єктів усіх форм власності;
- виявлення і розслідування кіберзлочинів.

Виявлення і блокування кібератак здійснює Європейська агенція мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), кібератаки виявляє підрозділ CERT-EU за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів ІТС з інформацією, яка захищається, та центру збору інформації про кібератаки. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається центр.

Виявлені CERT-EU кібератаки з ознаками злочинних дій чи розвідувально-підривних акцій передаються до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, EC3), який надалі може поінформувати про них Європейську агенцію оборони (European Defence Agency, EDA) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) для реагування дипломатичними каналами [16; 17].

ENISA, Європейське оборонне агентство (EDA), Європол та Група з реагування на комп’ютерні надзвичайні ситуації для установ, органів та установ ЄС (CERT-EU) 23 травня 2018 року підписали Меморандум про взаєморозуміння, яким встановили основи співпраці між їхніми організаціями. ENISA, EDA, EUROPOL та CERT-EU почали дискусії в 2016 році, що в підсумку призвело до підпису Меморандуму про взаєморозуміння [18]. Такий механізм співпраці може бути актуальним і для відповідних відомств в Україні.

У нашій державі передбачено (ст. 14 Закону України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 р.) можливість надання Україною іноземній державі інформації з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов’язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору. Подібні норми мають передбачати у національних правових системах й інші держави задля ефективної боротьби з транснаціональною кіберзлочинністю.

Насамкінець відзначимо, що у різних державах створюються спеціалізовані підрозділи правоохоронних органів для розслідування кіберзлочинів, збирання та аналізу електронних доказів. Адже з огляду на те, що робота з комп’ютерним

обладнанням вимагає спеціальних знань, кіберзлочини мають розслідуватись виключно співробітниками тих підрозділів правоохоронних органів, які мають спеціальні навички для ведення відповідних проваджень та пройшли підготовку.

Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін. Серед основних функцій цих підрозділів виділяють:

- моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;
- здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;
- розслідування кіберзлочинів, надання методичної та практичної допомоги іншим органам, зокрема правоохоронним у межах своєї компетенції;
- накопичення, узагальнення та аналіз інформації про кіберзлочинність;
- профілактика кіберзлочинів за допомогою громадськості та засобів масової інформації;
- навчання працівників поліції [15, с. 109].

Висновки.

Для покращення рівня співробітництва вітчизняних правоохоронних органів із зарубіжними партнерами доцільно створити в Україні єдиний технологічний центр обміну інформацією про кіберзагрози між правоохоронними органами України, ЄС та НАТО. Такий центр імовірно має бути створений на платформі співробітництва України з Інтерполом і Європолом, що сформована на базі Департаменту міжнародного поліцейського співробітництва Національної поліції України. Існує потреба провадження у вітчизняну практику взаємодії з правоохоронними органами іноземних держав типових формалізованих документів інформаційного обміну для негайної передачі державі-стороні, яка потерпіла від транснаціонального кіберзлочину, з використанням мережі національних контактних пунктів.

Ефективними з огляду на завдання боротьби з транснаціональною кіберзлочинністю є запровадження міждержавного обміну інформацією із закритих хакерських форумів, яку отримують в США, Нідерландах, Франції, Великобританії, Канаді, інших державах, а також використання ресурсів репозиторію “Cybercrime” щодо законодавства понад 180 країн про кіберзлочинність та електронні докази, судову практику, а також успішні правоохоронні операції.

Перспективами подальших наукових пошуків визначаємо питання співвідношення інституту персональних даних і таємниці слідства під час розслідування кіберзлочинів.

Використана література

1. Про кіберзлочинність : Конвенція Ради Європи від 21 листопада 2001 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575
2. Марущак А.І. Проблеми розслідування кіберзлочинів в Україні / Економіка. Фінанси. Право. – 2018. – № 1. – С. 23-27.
3. Global Programme on Cybercrime. URL: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
4. Cybercrime Repository. URL: https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html

5. The changing nature of cybercrime. URL: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

6. Interpol-led cybercrime operation across ASEAN unites public and private sectors. URL: https://www.interpol.int/News-and-media/News/2017/N2017-051

7. Building stronger international legal framework for cybercrime. URL: https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cyb ercrime

8. 153 detained for ticket fraud following worldwide law enforcement operation. URL: https://www.interpol.int/News-and-media/News/2017/N2017-078, 13 June 2017

9. Police around the world learn to fight global-scale cybercrime. URL: http://theconversation.com/police-around-the-world-learn-to-fight-global-scale-cybercrime-75804

10. Офіційні дані Департаменту кіберполіції НПУ.

11. Threat Assessment on Internet Facilitated Organised Crime (IOCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011

12. Massive blow to criminal Dark Web activities after globally coordinated operation. URL: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

13. Rolf van Wegberg and Thijmen Verburgh. 2018. Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In Proceedings of Workshop on the Evolution of the Darknet (WEBSCI). ACM, New York, NY, USA, 5 pages. URL: https://doi.org

14. Офіційні дані СБ України.

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

16. Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. – Brussels, 7.2.2013. – Join (2013) 1 final.

17. An evaluation Framework for National Cyber Security Strategies / Веб-сайт “European Union Agency for Network and Information Security”. URL: http://www.enisa.europa.eu

18. Four EU cybersecurity organisations enhance cooperation. URL: https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~