УДК 343.98, 343.34, 343:004.9

О. В. ОРЛОВ, Ю. М. ОНИЩЕНКО

МІЖНАРОДНА СПІВПРАЦЯ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННСТЮ

***Р**озглянуто питання надання взаємної міждержавної правової допомоги відносно кіберзлочинності як транснаціональної загрози. Надано пропозиції щодо поліпшення існуючих методів і створення нових підходів для координації міжнародної співпраці щодо боротьби з кіберзлочинністю.*

Ключові слова: кіберзлочин, кібербезпека, міжнародне співробітництво, загроза, запит.

***T**he paper considers issues of rendering mutual intergovernmental legal assistance concerning cybercrime as a transnational threat. Suggestions for improvement of the existing methods and new approaches to coordination of international cooperation in cybercrime control have been given.*

Key words: cybercrime. cyber security, international cooperation, threat, request.

Процес інформатизації сучасного суспільства спричинив те, що інформація перетворилася на своєрідний стратегічний ресурс, який володіє цінністю, тобто володіє якостями товару.

У свою чергу, впровадження сучасних технологій в економіці, управлінні, кредитово-банківській діяльності, стрімкий розвиток інформаційних і телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет і спрощення доступу до неї широкого кола користувачів через персональні комп'ютери зумовило зростання злочинних проявів у вказаній сфері.

Тенденція до розширення міжнародної співпраці в боротьбі зі злочинністю у сфері високих технологій наголошується в діяльності багатьох міжнародних організацій. Так, Рада Європи вважає, що без державного контролю комп'ютерних мереж обійтися не можна, а законодавче регулювання кіберпростору в одній окремо взятій країні навряд чи можливо.

Серед питань, пов'язаних з кіберзлочинністю, які в Україні вимагають негайного вирішення такі, як:

– термінологічна невизначеність;

– відсутність координації діяльності відповідних відомств;

– залежність України від програмних і технічних продуктів іноземного виробництва і складності з кадровим наповненням структурних підрозділів силових структур в державі;

– відсутність до сьогодні у нормативно-правових документах, у тому числі міжнародних загальновизначених понять термінів "кіберпростір", "кіберзлочинність", "кібертероризм" і "кібервійна", що дозволило б точніше визначити кордони суспільно небезпечного діяння, що підпадає під це поняття.

Боротьба з кіберзлочинністю лише в межах своєї держави малоефективна. Однак формування міжнародних механізмів йде дуже важко. Постійно постає питання про надання даних про кіберзлочини за рубіж.

За останні роки вже не раз поставало питання про вдосконалення міждержавного співробітництва у сфері боротьби зі злочинами з використанням нових інформаційних технологій. А. Широкова-Мурараш та Ю. Акчурін звертають увагу на висвітлення небезпеки безконтрольного використання інформативно-комунікативних технологій і визначення шляхів нормативного регулювання питань міжнародної інформаційної безпеки [10]. Є. Зозуля визначає, що ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур (і, щонайперше, правоохоронних органів) у розслідуванні такого роду злочинів [5]. На погляд І. Європіної, встановлення єдиних принципів і матеріально-правових основ з питань протидії кіберзлочинності є одним із найактуальніших. Такого роду неузгодженість базується на розбіжностях соціально-економічних, історичних умов розвитку країн і регіонів. Проте, зіштовхуючись із проявами транснаціональної злочинності, вироблення єдиної матеріально-правової концепції є обов'язковою умовою для провадження кооперації в контексті боротьби з кіберзлочинністю [3]. В. Марков відмічає, що в міжнародній діяльності контактних пунктів реагування на кіберзлочини є питання, які потребують негайного вирішення, наприклад внесення змін до чинного законодавства, щодо порядку та підстав виконання запитів отриманих від правоохоронних органів країн, у зв'язку з ратифікацією конвенції про кіберзлочинність [6]. В. Бабакін зазначає, що характер злочинів у сфері комп'ютерної інформації вимагає міждержавного підходу до протидії їм, ефективність якого недосяжна без міжнародного співробітництва. Одним з основних документів, що регулює порядок проведення розслідувань кіберзлочинів, є європейська Конвенція по боротьбі з кіберзлочинністю [1]. Важливим є положення Конвенції, яке дає можливість приймати законодавчі та інші заходи, які уповноважують її компетентні власті конфіскувати або подібним чином убезпечити від знищення дані які є у провайдера Інтернет і необхідні для розслідування кіберзлочинів [2].

Мета статті – розглянути питання надання взаємної міждержавної правової допомоги відносно кіберзлочинності як транснаціональної загрози. Надати пропозиції щодо поліпшення існуючих методів та створення нових підходів для координації міжнародної співпраці по боротьби з кіберзлочинністю.

Сучасні світові глобалізаційні процеси в поєднанні з інтенсивною інформатизацією зумовлюють низку динамічних явищ, які визначають пріоритетність напрямів державної політики у сфері забезпечення як національної безпеки в цілому, так і кожній з її складових. Сьогодні інформаційна сфера складає інтегруючу основу життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається одним з фундаментальних чинників в його подальшому розвитку. За таких умов особливого значення набуває нейтралізація негативного впливу і подолання суспільно небезпечних явищ, які мають прояви в інформаційній сфері, одним з яких є кіберзлочинність.

У багатьох країнах різке зростання кількості користувачів глобальною мережею Інтернет збігся за часом економічних і демографічних перетворень, зростанням розриву в доходах, скороченням витрат в приватному секторі і зниженням фінансової ліквідності. На загальносвітовому рівні правоохоронні органи відзначають зростання рівня кіберзлочинності у зв'язку з тим, що приватні особи, і організовані злочинні групи використовують нові інформаційні технології для

здійснення злочинів, керуючись прагненням до отримання вигоди. Для здійснення кіберзлочинів не потрібно знання складних методів. З'явилася субкультура молодих людей, що займаються фінансовим шахрайством за допомогою комп'ютерів. Багато з них почали займатися кіберзлочинністю в кінці підліткового віку.

У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються з метою отримання фінансової вигоди, злочини, пов'язані з використанням інформації, що знаходиться в комп'ютері, а також злочини, направлені проти конфіденційності, цілісності і доступності комп'ютерних систем.

Проте державні органи і підприємства приватного сектора по-різному сприймають відносний ризик і загрозу. У даний час статистичні дані про злочинність, що реєструються правоохоронними органами, не являють собою міцної основи для міждержавних порівнянь, хоча такі статистичні дані часто важливі для розробки політики на національному рівні. Показники кіберзлочинності, що реєструються правоохоронними органами різних країн, залежать не стільки від безпосереднього рівня злочинності, скільки від рівня розвитку країни і спеціалізованих можливостей підрозділу по боротьбі зі злочинами в галузі нових інформаційних технологій.

Кіберзлочини набувають транснаціонального характеру в тому випадку, якщо який-небудь елемент або наслідки злочину виявляються на території іншої країни або якщо частина скоєння злочину відбувається на території іншої країни.

Міжнародне право передбачає низку підстав для юрисдикції відносно таких діянь, у тому числі різні види юрисдикції за територіальним принципом і юрисдикцією на основі громадянства. Деякі з цих підстав закріплені в міжнародних документах із запобігання кіберзлочинності. Хоча всі країни Європи вважають, що національне законодавство забезпечує достатню основу для криміналізації і переслідування екстериторіальних кіберзлочинів, на наш погляд, що правова база до попередження таких видів злочинів є недостатньо розвиненою. У законодавстві багатьох країн знайшла віддзеркалення ідея про те, що для визнання територіальної юрисдикції всередині країни повинно бути здійснено не обов'язково "весь" злочин. Територіальна прив'язка може бути проведена відносно елементів або наслідків діяння, а також місця знаходження комп'ютерних систем або даних, які використовувалися для скоєння злочину. У разі виникнення юридичних конфліктів вони зазвичай вирішуються за допомогою проведення між країнами офіційних і неофіційних консультацій. Поки що відповіді країн не свідчать про яку-небудь необхідність у додаткових формах юрисдикції відносно якогось умовного виміру "кіберпростору".

Навпаки, форми юрисдикції за територіальною ознакою і на основі громадянства майже завжди здатні забезпечити достатній зв'язок між кіберзлочинами і хоч би однією державою.

Форми міжнародної співпраці включають видачу, надання взаємної правової допомоги, взаємне визнання іноземних судових рішень і неофіційну співпрацю між правоохоронними органами різних країн. Зважаючи на нестійкий характер електронних доказів у рамках міжнародної співпраці в кримінальних питаннях у області кіберзлочинності необхідне своєчасне представлення відповідей сфері наявність можливості поводитися з проханням про проведення спеціалізованих

слідчих дій, таких як збереження безпосередньо інформаційних і комп'ютерних даних, таких як лістинги логів, транзакції тощо. У питаннях отримання екстериторіальних доказів у контексті справ, пов'язаних з кіберзлочинами, переважають традиційні форми співпраці. Для цих цілей використовують офіційні прохання про надання взаємної правової допомоги. У рамках такого офіційного співробітництва, як правову основа використовуються двосторонні документи або багатосторонні документи про співпрацю. Останній приклад – Європейський центр боротьби з кіберзлочинністю (European CyberCrime Centre (EC3), який запрацював на початку 2013 р.

EC3 став координаційним центром ЄС у боротьбі з кіберзлочинністю. Країни – члени ЄС і європейські інституції мають намір підтримувати EC3 для створення оперативних і аналітичних можливостей розслідування кіберзлочинів і для співпраці з міжнародними партнерами.

Мандат діяльності Центру включає боротьбу з такими видами кіберзлочинності: злочини, здійснені організованими групами для отримання злочинних доходів, зокрема online-шахрайство; злочини, які завдали серйозної шкоди жертві, зокрема сексуальна експлуатація дітей; злочини, які завдали шкоди критично важливим інфраструктурним та інформаційним системам в ЄС [4].

Час представлення відповідей у рамках офіційних механізмів часто складає декілька місяців в разі прохань як про видачу, так і про надання взаємної правової допомоги. Такий термін створює проблеми в справі збору електронних доказів кіберзлочину.

На даний час Інтерпол визнається як офіційний канал для передачі прохань про тимчасовий арешт у багатьох двосторонніх і багатосторонніх угод про видачі, включаючи Європейську Угоду з видачі, Угоду з видачі Економічного співтовариства Західно-Африканських держав (ECOWAS) і Угоди в Організації Об'єднаних Націй щодо видачі злочинців [9].

Офіційні і неофіційні канали співпраці призначені для регулювання процесу отримання згоди держави на проведення іноземними правоохоронними органами розслідувань, що зачіпають суверенітет держави. Проте слідчі, свідомо або несвідомо, все частіше звертаються до екстериторіальних даних у процесі збору доказів, не просячи згоди держави, в якій фізично знаходяться ці дані. Ця ситуація виникає, зокрема, у зв'язку з хмарними комп'ютерними технологіями, що передбачають зберігання даних в декількох центрах даних в різних географічних точках.

Хоча "місцезнаходження" даних технічно може бути встановлене, воно набуває усе більш штучного характеру, аж до того, що навіть традиційні прохання про надання взаємної правової допомоги часто прямуватимуть у країну місця знаходження постачальника послуг, а не країну, в якій фізично розташовано центр передачі даних. Іноземні правоохоронні органи можуть використовувати прямий доступ до екстериторіальних даних у тих випадках, коли слідчі використовують існуюче "живе" підключення з пристрою підозрюваного або коли слідчі використовують отриманий законним чином дозвіл на доступ до даних. Слідчі правоохоронних органів інколи можуть отримувати дані від екстериторіальних постачальників послуг за допомогою неофіційного прямого запиту, хоча постачальники послуг зазвичай вимагають дотримання належної правової процедури. У відповідних положеннях про "трансграничний" доступ, що містяться в Конвенції про кіберзлочинність Ради Європи

і Конвенції про злочини в галузі інформаційних технологій Ліги арабських держав, такі ситуації враховуються не повною мірою, оскільки упор в них робиться на "згоду" особи, правомочної розкривати дані, і передбачається, що на момент доступу до даних або отримання даних відоме місце їх знаходження.

Зважаючи на теперішню ситуацію в галузі міжнародної співпраці, виникає ризик утворення міждержавних угрупувань, у рамках яких існують необхідні повноваження і процедури для співпраці між країнами, які входять в їх склад та по відношенню до всіх інших країн обмежуються "традиційними" видами міжнародної співпраці, що не враховують особливості електронних доказів і глобальний характер кіберзлочинності. Це особливо стосується співпраці при проведенні розслідувань. Відсутність загального підходу, у тому числі в рамках існуючих багатосторонніх договорів у сфері кіберзлочинності, означає, що можуть виникати труднощі у виконанні прохань про вживання таких заходів, як оперативне забезпечення збереження даних у країнах, що не входять до країн, що несуть міжнародні зобов'язання відносно забезпечення такого механізму і його задіювання в разі надходження запиту. Включення таких повноважень до проекту Конвенції про кібербезпеку Африканського союзу може в деякій мірі сприяти ліквідації цієї прогалини. З метою створення сприятливих умов для розвитку інформаційно-комунікаційних технологій, в рамках програми "Нове партнерство на користь розвитку Африки (НЕПАД) ООН співробітничає з Комісією Африканського союзу в розробці конвенції по кібербезпеку в Африці за зразком Конвенції про я :кіберзлочинність [7]. У всьому світі розбіжності у сфері обхвату положень відносно співпраці, що містяться в багатосторонніх або двосторонніх документах, відсутність зобов'язання представляти відповідь протягом певного терміну, відсутність домовленості про допустимий прямий доступ до екстериторіальних даних, великою кількістю неофіційних мереж правоохоронних органів і відмінності в гарантіях співпраці є серйозні проблеми у справі забезпечення ефективної міжнародного співробітництва в галузі електронних доказів по кримінальних справах.

Кіберзлочинність є міжнародною проблемою, оскільки об'єкти її посягання знаходяться в кіберпросторі, який необмежений державними кордонами.

У протидію з цим негативним явищем міжнародного характеру залучені всі держави світу, незалежно від рівня їх технічного розвитку і національного законодавства. При цьому менш розвинені в технічному відношенні країни мають можливість використовувати досвід розвинених країн для запобігання і розслідування комп'ютерних злочинів.

З уведенням в дію нового Кримінально-процесуального кодексу України 19 листопада 2012 р. значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про "Конвенцію про кіберзлочинність" і Закону України "Про міліцію", то зараз така інформація віднесена до категорії документів, що містять комерційну таємницю, яка охороняється законом (Глава 46 Цивільного Кодексу України) [8].

Таким чином, органи і підрозділи, на які покладені обов'язки по боротьбі з кіберзлочинністю, позбавлені можливості оперативно і своєчасно обробляти запити правоохоронних органів інших країн по збору доказів про кіберзлочини і встановлення місцезнаходження підозрюваних у рамках "Конвенції про кіберзлочинність".

З метою ефективної боротьби з кіберзлочинністю на національному і міжнародному рівнях, необхідно давати адекватну оцінку змінам процесуальних норм ведення розслідування і переслідування в судовому порядку, а також враховувати вимоги часу і потреби практики.

Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у тому числі і на законодавчому рівні. Тому, враховуючи вищевикладене, необхідно терміново підготувати і внести зміни до чинного законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів країн у рамках виконання зобов'язань України, узятих у зв'язку з ратифікацією "Конвенції про кіберзлочинність".

Для ефективної протидії кіберзлочинності необхідний інтегрований підхід, який можна забезпечити лише колективними зусиллями міжнародної спільноти через тісну взаємодію державних інститутів.

Література:

1. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV // ВВР України. – 2006. – № 5-6. – Ст. 71.

2. *Бабакін В. М.* Особливості міжнародного співробітництва при розслідуванні кіберзлочинів / В. М. Бабакін // Форум права. – 2011. – № 4. – С. 27–30 [Електронний ресурс]. – Режим доступу : http://archive.nbuv.gov.ua/e-journals/FP/2011-4/11bvmprk.pdf.

3. *Європіна І.В.* Практичні аспекти організації та провадження міжнародно-правової діяльності з протидії комп'ютерній злочинності / І. В. Європіна // Часопис Академії адвокатури України. – 2011 [Електронний ресурс]. – Режим доступу : http://*archive.nbuv.gov.ua/e-journals/Chaau/2011-2/11eivpkz.pdf.*

4. Євросоюз відкрив центр по боротьбі з кіберзлочинністю. Дзеркало тижня. Україна [Електронний ресурс]. – Режим доступу : http://dt.ua/TECHNOLOGIES/evrosoyuz_vidkriv_tsentr_po_borotbi_z_kiberzlochinnistyu.html.

5. *Зозуля Є. В.* Діяльність МВС України щодо протидії транснаціональній злочинності у сфері високих технологій / Є. В. Зозуля [Електронний ресурс]. – Режим доступу : http://archive.nbuv.gov.ua/portal/Soc_Gum/NZTNPU_ist/2011_1/Articles/35_Zozulya.pdf&sa=U&ei=mqFoUu_hLoHLtQbGgYHgAQ&ved=0CBgQFjAA&sig2=lGd-bg-Akv6v8HqZjSfctg&usg=AFQjCNG0Az9Uag_RzxKY_hzYQA3CqkcckA.

6. *Марков В. В.* Актуальні проблеми інформаційної безпеки України в системі міжнародної координації / В. В. Марков // Право і безпека. – 2013. – № (48). – С. 7–80.

7. ООН содействует подключению Африки к другим частям мира широкополосными подводными кабелями. Центр новостей ООН [Електронний ресурс]. – Режим доступу : http://www.un.org/russian/news/.

8. Право інтелектуальної власності на комерційну таємницю. Цивільний (гражданский) кодекс України [Електронний ресурс]. – Режим доступу : http://www.civilniy.org.ua/book4th/g46/default.htm.

9. *Старжинський В. С.* Інтерпол. Міжнародна організація кримінальної поліції : навч. посіб. / В. С. Старжинський, С. В. Старжинський, П. В. Хотенець. – Х. : Бурун Книга, 2006. – 112 с.

10. *Широкова-Мурараш О. Г.* Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-правовий аспект / О. Г. Широкова-Мурараш, Ю. Р. Акчуріна [Електронний ресурс]. – Режим доступу : http://poiskbook.kiev.ua/art/ipravo20112/ipavo-dwl.pdf.

Надійшла до редколегії 04.11.2013 р.