

УДК 341.4

**А. В. ВОЙЦІХОВСЬКИЙ,***кандидат юридичних наук, доцент,**доцент кафедри державно-правових дисциплін**факультету підготовки фахівців для підрозділів слідства та дізнання**Харківського національного університету внутрішніх справ***МІЖНАРОДНЕ СПІВРОБІТНИЦТВО В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ**

Висвітлено проблемні питання здійснення міжнародного співробітництва у боротьбі з кіберзлочинністю, досліджено міжнародно-правові та організаційні форми даної співпраці.

Широке використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому висуває вирішення проблем інформаційної безпеки в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини.

**Актуальність** даної теми статті обумовлена саме тим, що зростання інформаційних технологій зумовлює не тільки прогресивні зміни в економіці, але й негативні тенденції розвитку злочинного світу, появу нових форм і видів злочинних посягань. Це виявляється в тім, що зловмисники активно використовують у своїй злочинній діяльності новітні комп'ютерні засоби і нові інформаційні технології. Розповсюдження комп'ютерних вірусів і дитячої порнографії, шахрайство з пластиковими платіжними картками, розкрадання грошових коштів з банківських рахунків, комп'ютерний тероризм – це далеко не повний перелік злочинів, сукупність яких отримала широковживану назву «кіберзлочинність».

У сфері вирішення питань протистояння сучасним загрозам в інформаційній сфері продовжує залишатися актуальною тема розвитку співпраці правоохоронних органів різних держав.

Вивчення стану наукової розробленості проблем співпраці і взаємодії правоохоронних органів різних держав у боротьбі з кіберзлочинністю свідчить, що на сучасному етапі спеціального дослідження з цих проблем не проводилося. Проте необхідно відзначити, що окремі аспекти такої співпраці розглядалися в наукових роботах Ю. М. Батуріна, П. Д. Біленчука, В. Б. Вехова, В. О. Голубєва, М. Д. Діхтяренка, Б. Х. Толеубєкова і деяких інших.

**Метою** даної статті є комплексне вивчення проблем, пов'язаних із міжнародною співпрацею правоохоронних органів у боротьбі з кіберзлочинністю і на базі цього розроблення пропозицій щодо підвищення ефективності протистояння даним злочинам.

Інтернет як глобальна комп'ютерна мережа вже давно став притулком різних злочинців. Мережа, що об'єднала мільярди людей по всьому світу, надає унікальні можливості не тільки рядовим користувачам, але і зловмисникам. Завдяки анонімності і відсутності меж

Інтернет став ефективною зброєю в руках злочинців.

За оцінками експертів Міжнародної торгової палати, число злочинів, які вчиняються за допомогою глобальної комп'ютерної мережі Інтернет, зростає, причому пропорційно числу користувачів. За даними Інтерполу, Інтернет став тією сферою, де рівень злочинності зростає найшвидшими темпами [1, с. 41].

Враховуючи чинник глобалізації такого виду злочинності, очевидним стає те, що жодна держава вже не здатна самотійно протистояти цій небезпеці. У зв'язку з цим невідкладною проблемою стає активізація міжнародної співпраці в цій сфері. Істотне місце в такій співпраці належить міжнародно-правовим механізмам регулювання і взаємодії правоохоронних органів у питаннях протидії комп'ютерним злочинам.

Слід зазначити, що масове поширення кіберзлочинності почалося приблизно 20 років тому. Проте вже сьогодні широке застосування сучасних технологій разом із погано оснащеними органами комп'ютерної безпеки призвело до створення глобальної мережі кіберзлочинців. Дедалі більше ознак свідчить про те, що стосовно випадків злочинів у комп'ютерній сфері можна говорити про організовану злочинність.

Сьогодні проблема комп'ютерної злочинності досить гостро постає в США. За заявою директора Федерального бюро розслідування США, до десятки пріоритетних напрямів роботи відомства, разом з антитерористичною діяльністю і боротьбою з корупцією, тепер входить боротьба зі злочинами у сфері комп'ютерної інформації і захисту США від кібератак. Спеціальні органи постійно попереджають американські компанії про загрозу з боку хакерів, причому головним чином з Росії та України. Кіберзлочинці зламують сайти компаній, займаються торговими і фінансовими операціями в комп'ютерній мережі, викрадають номери пластикових карток клієнтів тощо.

Річні світові збитки від комп'ютерних злочинів становлять більше 5 млрд дол. США. За даними ООН, уже сьогодні збитки від комп'ютерних злочинів зрівняли з доходами від незаконного обігу наркотиків і зброї [2].

Можливості комп'ютерної мережі Інтернет інтенсивно освоює і наркомафія. Наркотогровці і їх клієнти дедалі частіше укладають угоди в «закритих кімнатах» каналів чату, захищених від сторонніх програмними засобами, і відми-

вають свої незаконні доходи в так званих інтернет-банках.

На сучасному етапі поняття «кіберзлочинність» є поки незвичним для правоохоронних органів, хоча злочинні дії, в яких використовуються комп'ютерна мережа, несуть у собі велику суспільну небезпеку. Вирішення даної проблеми, особливо з урахуванням її транснаціональної складової, дає підстави вважати, що розроблення загальної політики (стратегії) боротьби з кіберзлочинністю набуває сьогодні особливої актуальності для всіх держав.

На жаль, ступінь загрози, що несуть у собі комп'ютерні злочини, не до кінця ще усвідомлена й оцінена в суспільстві. Але навіть той незначний досвід, який вже є в цій галузі, а тим більше досвід найбільш розвинених країн світу, зі всією очевидністю свідчить про уразливість будь-якої держави, тим паче що кіберзлочинність не має державних кордонів, і злочинець здатний однаково загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі.

Особливу заклопотаність викликає проблема розслідування такого роду злочинів, оскільки їх сліди стираються або знищуються комп'ютерними злочинцями. Іншою особливістю кіберзлочинів, що ще більш ускладнює їх виявлення, є використання малогабаритних супутникових систем зв'язку, що дозволяють вчиняти злочини на значній відстані від об'єкта злочину буквально за частки секунди. При цьому розслідування таких злочинів може займати тижні, якщо не місяці, даючи злочинцю можливість знищити сліди злочину і уникнути покарання.

Для ефективного запобігання транснаціональним комп'ютерним злочинам необхідний узгоджений міжнародний підхід на різних рівнях. На національному рівні для розслідування кіберзлочинів потрібен добре підготовлений штат співробітників і вдосконалене національне законодавство з метою формування ефективною правовою основою для забезпечення слідчої, оперативної-розшукової діяльності правоохоронних органів і спецслужб у боротьбі з подібними злочинами. На міжнародному рівні необхідні оперативні дії, що спираються на координацію зусиль національних центрів із запобігання і розслідування транснаціональних комп'ютерних злочинів з аналогічними міжнародними центрами в інших країнах.

Хоча зацікавлені держави вже вирішують проблемні питання протидії транснаціональним комп'ютерним злочинам, на міждержавному

рівні такому виду злочинності ще не приділяється достатня увага. Причини відсутності уваги до кіберзлочинності можуть включати відносно низький рівень участі в міжнародних електронних комунікаціях, недостатній рівень досвіду в правоохоронній сфері і занижені оцінки соціальних втрат, яких можуть завдати комп'ютерні злочини. У рамках глобальної комп'ютерної мережі кримінально-правова політика окремої держави завдає прямого впливу на міжнародне співтовариство. Кіберзлочинці можуть учиняти свої дії в інформаційному середовищі через певну державу, де такі дії не криміналізовані, і таким чином вони можуть знаходитися під «захистом» закону такої країни. Отже, забезпечення міжнародної співпраці правоохоронних і судових органів різних держав неможливе без узгодження й ухвалення норм кримінального права відносно кіберзлочинів в окремих державах [3].

Одним із найсерйозніших кроків, спрямованих на врегулювання цієї проблеми, є прийняття Радою Європи 23 листопада 2001 р. Конвенції про кіберзлочинність (набула чинності 1 липня 2004 р.). Документ підписали 29 держав, у тому числі Україна (ратифікувала 7 вересня 2005 р. [4]). Конвенція про кіберзлочинність (далі – Конвенція) є першим міжнародним договором у галузі протидії злочинам, що вчиняються через комп'ютерні мережі.

Основною метою Конвенції про кіберзлочинність є проведення в пріоритетному порядку загальної політики у сфері кримінального права, спрямованої на захист суспільства від комп'ютерних злочинів, зокрема шляхом ухвалення відповідних законодавчих актів і зміцнення міжнародної співпраці.

Конвенція стала результатом спільної роботи експертів Ради Європи за участю США, Канади, Японії та інших країн, які не є членами Організації. Згодом до Конвенції був підготовлений Додатковий протокол, що передбачає кримінальну відповідальність за публікацію расистської або ксенофобської пропаганди через комп'ютерні мережі [5] (ратифікований Україною 21 липня 2006 р. [4]).

Розглядаючи питання протидії кіберзлочинності через призму Конвенції, можна дати оцінку цього документа і визначити його міжнародне значення для вирішення даної проблеми. Одним із головних висновків, який можна зробити при аналізі Конвенції, – це те, що була вироблена загальна позиція з питання про те, які

діяння, пов'язані з використанням комп'ютерних систем, повинні визнаватися злочинними (злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем).

По-перше, такі дії вважаються злочинними і допускають застосування заходів, необхідних для виявлення, розслідування і судового переслідування таких злочинів, як усередині держави, так і на міжнародному рівні.

По-друге, наявність у Конвенції статті «Пошук і конфіскація збережених комп'ютерних даних» дають можливість одній стороні домогтися збереження важливої інформації, необхідної для розслідування злочину, яка знаходиться в юрисдикції іншої сторони. Такі дані зберігаються звичайно протягом обмеженого періоду часу, залежного від комерційних потреб оператора або постачальника послуг, а також юридичних вимог, що стосуються нерозголошення приватної інформації. Безперечно, такі положення Конвенції дозволять правоохоронним органам більш ефективно проводити розслідування комп'ютерних злочинів.

З правової точки зору велике значення мають і загальні принципи Конвенції, що стосуються міжнародної співпраці. Це питання видачі комп'ютерних злочинців і надання широкої взаємної правової допомоги при розслідуванні кримінальних справ, у тому числі збирання електронних доказів [6].

Проте не можна не відзначити і деякі складнощі в реалізації положень Конвенції про кіберзлочинність. Враховуючи те, що Конвенція набула чинності 1 липня 2004 р., на сьогодні її підписали лише 29 держав, а ратифікували – 14, можна стверджувати, що такий стан справ, природно, не дозволяє протистояти комп'ютерним злочинам всією світовою спільнотою.

Особливу роль у вирішенні проблем міжнародної співпраці в боротьбі з кіберзлочинністю відіграє Організація Об'єднаних Націй, у рамках якої неодноразово обговорювалися питання запобігання злочинам, пов'язаним із застосуванням комп'ютерних технологій, і боротьби з ними.

Ще у 2003 р. Генеральна асамблея ООН резолюцією 58/138 виразила свою заклопотаність зростанням злочинності у сфері інформаційних технологій. У резолюції особливо підкреслювався транснаціональний характер таких злочинів і необхідність вживання скоординованих у світовому масштабі заходів для запобігання їм і їх розслідування.

У рамках 11-ої (18–25 квітня 2005 р., Таїланд) і 12-ої (12–19 квітня 2010 р., Бразилія) Конгресів ООН із запобігання злочинності і кримінального правосуддя (UN Congress on Crime Prevention and Criminal Justice) обговорювалися проблемні питання міжнародного співробітництва в боротьбі з кіберзлочинністю. Учасники Конгресів обговорювали заходи щодо інтенсифікації міжнародної співпраці і вдосконалення національного законодавства у сфері боротьби з відмиванням грошей, торгівлі наркотиками, міжнародним тероризмом і кіберзлочинністю. Таким чином, ООН поставило комп'ютерні злочини в один ряд з міжнародним тероризмом, що свідчить про особливу увагу до даної проблеми з боку світової спільноти [7; 8].

У травні 2011 р. Міжнародний союз електророз'язку та Управління ООН з наркотиків і злочинності підписали угоду про боротьбу з кіберзлочинністю. Тепер ці організації мають намір зайнятися розробленням правових рамок і юридичних механізмів протидії загрозам у комп'ютерних мережах.

Першим кроком впровадження такої спільної ініціативи стало навчання більше 200 фахівців і 50 поліцейських основам забезпечення кібербезпеки і відстежування незаконної діяльності в Інтернеті [9].

Для прийняття конкретних заходів, спрямованих на обмеження комп'ютерних загроз, Організація Об'єднаних Націй розробила Глобальну програму кібербезпеки, Основні правила для дітей щодо їх захисту в онлайн-овому середовищі, Основні правила для батьків, опікунів і вчителів щодо захисту дитини в онлайн-овому середовищі, Основні правила для директивних органів щодо захисту дитини в онлайн-овому середовищі, Елементи для створення глобальної культури кібербезпеки тощо [10].

Окремі питання запобігання і розслідування подібних злочинів активно обговорюються в рамках ЮНЕСКО і Міжнародного телекомунікаційного союзу. Цими ж питаннями частково займається Робоча група з управління Інтернетом (WGIG) [11].

Враховуючи зростаючу небезпеку комп'ютерних злочинів для міжнародного співтовариства, Європейське поліцейське відомство (Європол) представило стратегію щодо вирішення проблем протидії кіберзлочинності. За оцінкою Європолу, кіберзлочинність за своєю природою не має меж, що ускладнює кримінальні розслідування в цій сфері, саме тому європей-

ським країнам необхідно тісніше співпрацювати між собою.

Європол має намір представити членам ЄС систему IOCTA (Internet Facilitated Organised Crime Tread Assessment), яка сприятиме розкриттю цілої низки злочинів, зокрема кіберзлочинів. На даний час Європол надає членам ЄС слідчу і аналітичну підтримку через свою систему онлайн-розслідувань і базу даних злочинів. Проте зараз тут говорять про швидке завершення роботи над системами Internet Crime Reporting Online System (ICROS) і Internet&Forensic Expert Forum (IFOREX). Ці системи надаватимуть можливість централізованої координації і загальних звітів від різних поліцейських національних європейських відомств [12].

У січні 2004 р. в ЄС розпочало роботу агентство з безпеки інформації і комп'ютерних мереж. Мета агентства – боротьба з комп'ютерним піратством і забезпечення швидкого обміну інформацією між країнами ЄС при появі подібних загроз. За допомогою агентства планується посилити безпеку комп'ютерних мереж, а також здатність країн ЄС запобігати атакам хакерів.

Прикладом одного із напрямків співпраці в боротьбі з кіберзлочинністю в рамках Європолу можуть послужити щорічні зустрічі керівників поліцейських відомств Європи. У червні 2011 р. на запрошення Європолу до Штабквартири організації прибула також делегація МВС України. На зустрічі обговорювалися питання, що стосуються стану співпраці в боротьбі з міжнародною організованою злочинністю, а саме з незаконним обігом наркотиків, торгівлею людьми, нелегальною міграцією, фінансовими злочинами і злочинами у сфері комп'ютерних технологій [13].

Останнім часом питання забезпечення інформаційної безпеки стають дедалі більш актуальними і для України. Про необхідність зміцнення інформаційного суверенітету держави як однієї з складових національної безпеки України говориться в Стратегії національної безпеки України, яка була затверджена Указом Президента України 12 лютого 2007 р. [14]. Зокрема, в п. 2.8 стратегії зазначено, що в даний час посилюється негативний зовнішній вплив на інформаційний простір України, що, у свою чергу, загрожує розмиванням суспільних цінностей і національної ідентичності; наближається до критичного стану безпеки інформаційно-комп'ютерних систем у галузі державного

управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх і міжнародних комунікацій тощо. У зв'язку з цим необхідно забезпечити сприятливі зовнішні умови для розвитку і безпеки держави, яка передбачає, зокрема, і забезпечення інформаційної безпеки при інтеграції в структури глобального інформаційного суспільства [14].

У процесі проведення розслідувань правоохоронні органи різних держав можуть співпрацювати між собою як офіційно, наприклад, використовуючи Інтерпол і Європол, так і неофіційно, надаючи потенційно корисну інформацію безпосередньо правоохоронним органам іншої держави. У зв'язку з правовою допомогою при розслідуванні кіберзлочинів неминуче виникатимуть і інші додаткові проблеми. Якщо внутрішнім правом однієї зі сторін не передбачені конкретні повноваження щодо пошуку доказів в електронному середовищі, така сторона не в змозі буде адекватно реагувати на прохання про надання допомоги. З цієї причини важливою умовою міжнародної співпраці є узгодження повноважень щодо вживання необхідних заходів для розслідування таких видів злочинів.

Одним із вирішальних чинників у боротьбі з кіберзлочинністю повинна стати не тільки ратифікація Конвенції окремими державами, але і гармонізація національного законодавства з урахуванням основних положень конвенції, тобто вироблення правових механізмів на національному рівні. Обмеженість національного законодавства і відсутність єдиної правової бази правоохоронних органів у боротьбі з цим видом правопорушень є однією з основних причин стрімкого зростання кількості таких злочинів.

Необхідно підкреслити, що важливою складовою стратегії протидії кіберзлочинності повинна стати міжнародна співпраця в цій галузі, оскільки вже очевидно, що протидіяти цим загрозам на рівні окремих держав практично неможливо. Така міжнародна співпраця в боротьбі зі злочинністю у сфері використання комп'ютерних технологій має потребу в наявності правового, організаційного і наукового забезпечення. Це той комплекс проблем, який потрібно невідкладно вирішувати міжнародним співтовариством у сфері боротьби з кіберзлочинністю в XXI ст.

#### Список використаної літератури

1. Селико Ю. Internet – отмычка для компьютера / Ю. Селико, А. Прохоров // Компьютер-пресс. – 2002. – № 3. – С. 40–43.
2. Зинина У. В. Международное сотрудничество в сфере борьбы с компьютерными преступлениями [Электронный ресурс] / Зинина У. В. // Право и безопасность. – 2005. – № 3 (16). – Режим доступа: [http://www.dpr.ru/pravo\\_16\\_19.htm](http://www.dpr.ru/pravo_16_19.htm).
3. Голубев В. Международному сотрудничеству в борьбе киберпреступностью – нет альтернативы [Электронный ресурс] / В. Голубев. – Режим доступа: <http://www.crime-research.ru/articles/golubev030205>.
4. Про ратифікацію Конвенції про кіберзлочинність : закон України від 7 верес. 2005 р. № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.
5. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [Електронний ресурс]. – Режим доступу: [http://www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994\\_687](http://www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_687).
6. Конвенція про кіберзлочинність від 23 листоп. 2001 р. [Електронний ресурс]. – Режим доступу: [http://zakon2.rada.gov.ua/laws/show/994\\_575](http://zakon2.rada.gov.ua/laws/show/994_575).
7. Одиннадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. – Режим доступа: <http://www.un.org/russian/events/11thcongress/index.html>.
8. Двенадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. – Режим доступа: <http://www.un.org/ru/conf/crimecongress2010>.
9. Агентства ООН объединились против киберпреступности [Электронный ресурс]. – Режим доступа: <http://www.unmultimedia.org/radio/russian/detail/84626.html>.
10. Кибербезопасность [Электронный ресурс] / Международный союз электросвязи. – Режим доступа: <http://www.un.org/ru/ecosoc/itu/cybersecurity.shtml>.
11. ООН ставит киберпреступность в один ряд с международным терроризмом [Электронный ресурс] // Информационное общество и общества знаний: новости, события, комментарии, аналитика. – Режим доступа: <http://www.ifar.ru/pr/2005/050427b.htm>.
12. Агентство Европол призывает к сотрудничеству в борьбе с киберпреступностью [Электронный ресурс]. – Режим доступа: <http://www.iso27000.listkom.ru/novosti-i-sobytiya/agenstvo-evropol-prizyvaet-k-sotrudnichestvu-v-borbe-s-kiberprestupnostyu>.
13. Анатолій Могильов взяв участь у 3'їзді керівників поліцій держав Європи // Іменем закону. – 2001. – № 27 (5777).

14. Стратегія національної безпеки України [Електронний ресурс] : указ Президента України від 12 лют. 2007 р. № 105/2007. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/105/2007>.

*Надійшла до редколегії 22.10.2011*

**ВОЙЦИХОВСКИЙ А. В. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ  
С КИБЕРПРЕСТУПНОСТЬЮ**

Освещены проблемные вопросы осуществления международного сотрудничества в борьбе с киберпреступностью, исследованы международно-правовые и организационные формы данного сотрудничества.

**VOYTSIKHOVSKYI A. INTERNATIONAL COOPERATION IN CYBERCRIME  
COMBATING**

The problem questions of realization of the international cooperation in combating cybercriminality, international legal and organizational forms of the given cooperation are researched.

---