УДК 343:004.9

В. ХАХАНОВСЬКИЙ, *кандидат юридичних наук, доцент*

КІБЕРЗЛОЧИННІСТЬ: ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ПРИ ВЧИНЕННІ ЗЛОЧИНІВ – ПРОБЛЕМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА МІЖНАРОДНОЇ СПІВПРАЦІ

Анотація. *Щодо стану та перспектив взаємодії МВС України з правоохоронними органами інших країн у боротьбі з комп'ютерною злочинністю.*

Правоохоронна практика свідчить, що останнім часом в усьому світі спостерігається значне зростання рівня злочинних актів щодо інформаційних систем, що являє загрозу як окремим організаціям, установам та фізичним особам, так й економіці кожної країни та суспільства в цілому.

Конвенцією про кіберзлочинність від 23 листопада 2001 року [1] передбачається надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях, укладення домовленостей щодо дієвого міжнародного співробітництва.

Згідно із зазначеною Конвенцією сторони співробітничають шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, а також внутрішньодержавного законодавства з метою розслідування або переслідування кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, збирання доказів у електронній формі.

Конвенцією про кіберзлочинність передбачено конкретні принципи міжнародного співробітництва, а саме:

- *термінове збереження комп’ютерних даних*. Будь-яка сторона може запитати іншу видати ордер чи іншим чином провести термінове збереження комп’ютерних даних за допомогою комп’ютерної системи, яка знаходиться на території іншої сторони, до якої сторона, яка запитує, збирається надіслати запит про взаємну допомогу щодо обшуку, доступу, арешту тощо або розголошення таких даних;
- *термінове розкриття збережених даних про рух інформації*. Якщо в ході виконання запиту щодо збереження даних про рух інформації, які стосуються конкретної передачі інформації, стороні, яку запитують, стає відомо, що постачальник послуг в іншій країні був залучений до передачі такої інформації, сторона, яку запитують, терміново повідомляє стороні, яка запитує, обсяг інформації про рух даних, достатній для ідентифікації такого постачальника послуг і шляху передачі цієї інформації;
- *взаємна допомога щодо доступу до комп’ютерних даних, які зберігаються*. Будь-яка сторона може запитати іншу провести обшук чи подібний доступ, арешт чи подібні дії або розголошення даних, які зберігаються за допомогою комп’ютерної системи, яка знаходиться на території сторони, яку запитують;
- *транскордонний доступ до комп’ютерних даних, які зберігаються (за згодою або у випадку, коли вони є публічно доступними)*. Будь-яка сторона може, не отримуючи дозволу іншої, здійснювати: доступ до публічно доступних (відкритих) комп’ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно; здійснювати доступ або

відновлювати за допомогою комп’ютерної системи, яка знаходиться на її території, комп’ютерні дані, які зберігаються і знаходяться в іншої сторони, якщо сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані цій стороні за допомогою такої комп’ютерної системи;

- *взаємна допомога у збиранні даних про рух інформації в реальному масштабі часу*. Сторони надають взаємну допомогу щодо збирання даних про рух інформації в реальному масштабі часу, пов’язаних із зазначеною передачею інформації на їх території, яка передається за допомогою комп’ютерної системи. Допомога регулюється умовами і процедурами, передбаченими внутрішньодержавним законодавством. Кожна сторона надає таку допомогу щонайменше відносно кримінальних правопорушень, стосовно яких проводиться збирання даних про рух інформації в реальному масштабі часу в разі подібної внутрішньодержавної справи;
- *взаємна допомога у перехопленні даних (змісту інформації)*. Сторони надають взаємну допомогу щодо перехоплення даних у зазначених комп’ютерних системах в обсягах, які дозволяються відповідними договорами та внутрішньодержавним законодавством.

Слід зазначити, що фахівці Департаменту державної служби боротьби з економічною злочинністю МВС України вважають за необхідне привести організацію взаємодії у відповідність до положень Конвенції про кіберзлочинність.

У 2004 році Міністерство закордонних справ України на виконання доручення Кабінету Міністрів України від 31.10.2003 р. № 69490 узгодило з Управлінням ООН з наркотиків і злочинності питання щодо проекту “Боротьба з організованою злочинністю в Україні шляхом запобігання махінаціям з кредитними картками та іншим фінансовим злочинам, пов'язаним з комп'ютерними технологіями”, відповідно до якого передбачалося проведення тренувальних семінарів для працівників правоохоронних органів і прокуратури, судових органів, банківських установ та поточні консультації з конкретних питань виявлення і переслідування злочинів у сфері зловживань з банківськими кредитними картками та інших злочинів, пов’язаних з комп'ютерними технологіями, а також семінар з оцінки законодавства у цій сфері.

В рамках реалізації зазначеного проекту ООН на виконання доручення Кабінету Міністрів України від 09.09. 2004 р. № 69490/01/1-03 у МВС України було утворено міжвідомчу робочу групу з проведення аналізу законодавства у сфері протидії і запобігання махінаціям з банківськими кредитними картками та іншим фінансовим злочинам, пов'язаним з комп'ютерними технологіями, та надання узгоджених пропозицій з його удосконалення.

До складу робочої групи увійшли фахівці: Управління взаємодії, координації та методичного забезпечення системи фінансового моніторингу, Аналітичного управління Державного департаменту фінансового моніторингу; Юридичного управління, Академії суддів України Державної судової адміністрації України; Головного управління податкової міліції, Департаменту боротьби з відмиванням доходів, одержаних злочинним шляхом, Державної податкової адміністрації України; Департаменту контррозвідувального захисту економіки держави, Головного управління боротьби з корупцією та організованою злочинністю Служби безпеки України; Департаменту Державної служби боротьби з економічною злочинністю та Головного управління боротьби з організованою злочинністю Міністерства внутрішніх справ України.

За результатами розгляду проекту ООН членами робочої групи було прийнято рішення про його доопрацювання, розроблено програму діяльності робочої групи для ви-

значення основних напрямів аналізу чинного законодавства, програму заходів з приведення чинного законодавства України у відповідність до міжнародних стандартів у сфері боротьби із шахрайством з кредитними картками та іншими фінансовими злочинами, пов‘язаними з комп‘ютерними технологіями, визначити в реалізації програми ступінь участі зацікавлених відомств відповідно до їх компетенції.

Членами міжвідомчої робочої групи протягом 2004-2005 років проведено певну роботу з удосконалення відповідних норм права, вивчені проблемні питання розробки нових методик боротьби зі злочинністю, пов'язаною із цією категорією злочинів. Зокрема, завдяки цій роботі в зазначений період Верховною Радою України прийнято:

– Закон України від 7 вересня 2005 року “Про ратифікацію Конвенції про кіберзлочинність” [2];

– Закон України від 6 жовтня 2004 року “Про внесення змін до Закону України “Про платіжні системи та переказ грошей в Україні” [3];

– Закон України від 23 грудня 2004 року “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” (щодо відповідальності за комп’ютерні злочини) [4];

– Закон України від 31 травня 2005 року “Про внесення змін до Закону України “Про захист інформації в автоматизованих системах” [5].

На розгляд Верховної Ради України направлено законопроект “Про внесення змін до деяких законів України (щодо управління ризиками, вимог безпеки до здійснення операцій з платіжними картками та іншими платіжними інструментами та покарання за злочини з їх використанням)” від 23.08.2005 року № 8035, яким передбачаються формування єдиної системи моніторингу за операціями, що здійснені з викраденими та підробленими платіжними картками, а також зміни до статті 200 КК України.

Разом з тим, угодою про співробітництво держав-членів СНД у боротьбі із злочинами у сфері комп'ютерної інформації (Мінськ, 1 червня 2001 року) передбачаються такі форми співпраці:

а) обмін інформацією, у тому числі про:

- злочини, які готуються або вчинені у сфері комп'ютерної інформації, та причетних до них фізичних і юридичних осіб;
- форми та методи попередження, виявлення, припинення, розкриття та розслідування злочинів у цій сфері;
- способи вчинення злочинів у сфері комп'ютерної інформації;
- національне законодавство та міжнародні договори, що регулюють питання попередження, виявлення, припинення, розкриття та розслідування злочинів у сфері комп'ютерної інформації;

б) виконання запитів про проведення оперативно-розшукових заходів, а також процесуальних дій відповідно до міжнародних договорів.

На ефективність співробітництва у сфері оперативно-розшукової діяльності негативно впливають невирішені проблеми своєчасного та повного обміну оперативною інформацією, недосконаліть нормативної бази з окремих напрямів діяльності. Потребує подальшого удосконалення механізм оперативного обміну інформацією про громадян, які затримувалися на території інших держав за злочини, пов’язані з використанням підроблених або викрадених платіжних пластикових карток банківських установ, шахрайством в мережі Інтернет, незаконним проникненням у комп'ютерні бази даних міністерств та

відомств, для перевірки на причетність до вчинення злочинів у сфері банківської діяльності та високих технологій.

На міжнародній практичній конференції по боротьбі з кіберзлочинністю та кібертероризмом (Москва, 19-20 квітня 2006 рік) МВС Росії запропонувало здійснити проект під назвою **“**Чиста мережа**”** (Clean net), метою якого є розробка та реалізація практичних заходів з протидії використанню мережі Інтернет у терористичних цілях, очищення глобального інформаційного простору від ресурсів, які негативно впливають на суспільну та індивідуальну свідомість і провокують екстремістські та терористичні прояви. Зокрема, пропонується: організувати виявлення та вивчення Інтернет-ресурсів, зміст яких направлено на пропаганду тероризму та його ідеології, розпалення міжнаціональної, релігійної ворожнечі; розробити загальні критерії визнання сайтів терористичними, удосконалити національні законодавства в бік їх гармонізації; розробити понятійний апарат в області боротьби з кібертероризмом, організувати обмін інформацією між правоохоронними органами про функціонування терористичних сайтів в Інтернет-просторі; поєднати зусилля держав та бізнес-спільнот різних країн з розробки та прийняття єдиних вимог до термінів зберігання даних Інтернет-провайдерами при наданні телематичних послуг на період до трьох років.

Для забезпечення ефективної боротьби з комп’ютерним шахрайством як найбільш поширеним видом злочинної діяльності в телекомунікаційних мережах, який заподіює значну шкоду економічним інтересам держав та громадян, ініційовано також проект під назвою “Чистий код” (Clean code). В рамках проекту правоохоронним органам інших країн запропоновано:

- здійснювати обмін інформацією про існуючі та нововиявлені схеми і способи вчинення комп’ютерних шахрайств, методиками їх виявлення та розслідування;
- вживати заходів щодо забезпечення збереження відомостей про приватних осіб, державні та комерційні організації, які потерпіли від комп'ютерного шахрайства;
- сприяти при виявленні транскордонних злочинів партнерам у збиранні доказів, встановленню та припиненню комп’ютерного шахрайства і притягненню до відповідальності осіб, причетних до його вчинення;
- розширювати співробітництво з провайдерами і банківськими установами в інтересах посилення безпеки систем електронних розрахунків та торгівлі, а також ефективного розслідування випадків комп’ютерного шахрайства, фіксації доказів та документування протиправної діяльності;
- використовувати для обміну інформацією канали міжнародної мережі національних контактних пунктів Інтерполу, а також апарати представників.

Крім того, ініційовано проект “Чисте з’єднання” (Clean connecting), яким передбачається удосконалення роботи мережі національних контактних пунктів 24/7 і пропонується країнам-учасникам:

- сприяти розширенню міжнародної мережі національних контактних пунктів за рахунок приєднання нових країн-учасників;
- вжити заходів щодо формування національних правових механізмів, які б забезпечували обмін оперативною інформацією з правоохоронними органами інших країн.

Пропонується також визначити перелік видів транскордонних комп'ютерних злочинів, інформація про вчинення яких повинна невідкладно направлятися правоохоронним органам потерпілої сторони каналами мережі національних контактних пунктів; запровадити в практику роботи національних контактних пунктів типові формалізовані

документи; визначити припустимі строки виконання запитів та надання відповідей їх ініціаторам у межах до 30 діб.

Як перший крок посилення ефективності боротьби з комп’ютерним шахрайством МВС Росії починає з 2006 року розповсюдження каналами мережі національних контактних пунктів інформації про виявлені та розслідувані в Росії факти комп'ютерного шахрайства з додаванням типових схем вчинення подібних злочинів.

Органами внутрішніх справ України при розкритті транскордорнних злочинів, для обміну інформацією з правоохоронними органами інших країн використовуються канали Інтерполу, міжнародної мережі національних контактних пунктів 24/7 (у структурі НЦБ Інтерполу), а також Управління міжнародних зв'язків МВС України, апаратів представників правоохоронних органів.

Сьогодні в Україні працюють представники МВС Австрійської Республіки, Королівства Бельгії, Республіки Білорусь, Федеративної Республіки Німеччини, Республіки Польща, Французької Республіки, Чеської Республіки, Королівства Данії. Відповідальний за Україну представник поліції держави Ізраїль знаходиться у Москві (Російська Федерація), представник поліції та митниці Королівства Швеції – у Будапешті (Угорщина). Представники МВС України за кордоном знаходяться в Республіці Польща, Федеративній Республіці Німеччини, державі Ізраїль. Забезпеченню повноти та швидкості розслідування кримінальних справ сприяла конструктивна взаємодія відділу боротьби з правопорушеннями у сфері високих технологій ДДСБЕЗ МВС України з Управлінням “К”, Бюро спеціальних технічних заходів МВС Росії та Управлінням спеціальних технічних заходів ГУМВС Санкт-Петербургу та Ленінградської області.

Щодо Національного центрального бюро Інтерполу, яке виступає центром координації взаємодії правоохоронних органів країни з компетентними органами зарубіжних держав, то, на жаль, його можливості не враховують специфіки виявлення та документування злочинної діяльності у сфері інформаційно-телекомунікаційних технологій. Так, при проведенні у 2003 році перевірки осіб, причетних до вчинення шахрайських дій з використанням підроблених електронних документів, каналами Інтерполу від правоохоронних органів США запитано інформацію про факт реєстрації, власників та керівників фірми, яка задіяна у шахрайській схемі та зареєстрована в США. Відповідь щодо підтвердження факту реєстрації фірми було отримано лише через півроку. Інформації щодо осіб, які її зареєстрували, не надано взагалі у зв’язку “із знаходженням відомостей про це в іншому відомстві”.

Для того щоб інформація з інших країн швидко та у доступній формі (мова повідомлення, специфічні терміни, коди злочинів тощо) надходила до національних спеціалізованих підрозділів, а також для оперативного обміну такою інформацією між країнами, Генеральний Секретаріат Інтерполу ще у 1994 році рекомендував державам-членам організації створити Національний центральний консультативний пункт з проблем комп'ютерної злочинності. В Україні такий пункт було створено у 1996 році на базі НЦБ Інтерполу.

Сьогодні взаємодія МВС України з правоохоронними органами інших країн у боротьбі з комп'ютерною злочинністю забезпечується за такими напрямами:

1. Проведення зустрічей керівників спеціалізованих підрозділів по боротьбі з високотехнологічною злочинністю для:

— координації роботи по попередженню, виявленню, припиненню та розкриттю комп'ютерних злочинів;

— вирішення питань практичної взаємодії підрозділів за напрямами роботи;

– узгодження питань спільного проведення наукових досліджень, розробок і програм з актуальних проблем, що становлять взаємний інтерес;

– ознайомлення з організаційною структурою спеціалізованих підрозділів по боротьбі зі злочинністю у сфері високих технологій; формами та методами роботи спеціалізованих підрозділів; позитивним досвідом діяльності у сфері попередження цього виду злочинності та боротьби з нею.

2. Підготовка, перепідготовка та підвищення кваліфікації кадрів спеціалізованих підрозділів з питань протидії комп’ютерній злочинності.

3. Обмін інформацією (за досягнутими домовленостями):

– оперативно-розшуковою, оперативно-довідковою, криміналістичною інформацією про комп'ютерні злочини, осіб, причетних до їх вчинення, а також аналітичною та архівною інформацією;

– законодавчими і нормативними актами, навчально-методичною літературою з питань діяльності спеціалізованих підрозділів.

Розробка ефективних форм взаємодії триває.

Використана література

1. Конвенція Ради Європи № 185 від 23.11.2001 р. “Про кіберзлочинність” *//www.conventions coe.int/treaty/en/Treaty/EN/Projets/cyber(draft).htm* (переклад див. у кн.: Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв’язку з автоматизованою обробкою даних у правоохоронній діяльності: Посібник. Книга 2 / Упорядники: М.Швець, В.Брижко, Б.Романюк, В.Цимбалюк; За ред. члена-кореспондента АПрН України М.Швеця та к.ю.н. Б.Романюка. – К.: НДЦПІ АПрН України, 2006 р. – С. 116-133).

2. Закон України від 7 вересня 2005 року “Про ратифікацію Конвенції про кіберзлочинність” //zakon.rada.gov.ua.

3. Закон України від 6 жовтня 2004 року № 2056-IV “Про внесення змін до Закону України "Про платіжні системи та переказ грошей в Україні” //zakon.rada.gov.ua.cgi-bin.laws.main.cgi?page= 8&user=1161845182584332.

4. Закон України від 23 грудня 2004 року № 2289-IV “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” //zakon.rada.gov.ua.cgi-bin.laws.main.cgi?page= 10&user=1161845182584332.

5. Закон України від 31 травня 2005 року № 2594-IV “Про внесення змін до Закону України “Про захист інформації в автоматизованих системах” //zakon.rada.gov.ua.cgi-bin.laws.main.cgi?page=11&user=1161845182584332.

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