ISSN 1995-6134

УДК 341.4
В.М. БАБАКІН, канд. юрид. наук, Харківський національний університет внутрішніх справ

ОСОБЛИВОСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Ключові слова: *кіберзлочини, транснаціональна злочинність, міжнародна співпраця, Конвенція по боротьбі з кіберзлочинністю*

Злочини у сфері комп'ютерної інформації мають динамічний характер. В результаті швидкого розвитку нових технологій не менш швидкими темпами з'являються нові форми комп'ютерної злочинності, які отримують поширення при використанні нових методів, наприклад, технології Bluetooth, бездротових мереж зв'язку Wi-Fi та WiMAX, пірингових мереж (P2P), спаму та інших.

За своєю суттю злочини у сфері комп'ютерної інформації є транскордонними, і тому всі міжнародні організації закликають держави у співпраці з іншими зацікавленими сторонами розробляти необхідне законодавство, що передбачає проведення спільних розслідувань зазначених діянь з використанням існуючого міжнародного права, і, зокрема, Конвенції Ради Європи з кіберзлочинності.

Все вище викладене підтверджує необхідність вдосконалення кримінального та кримінально-процесуального законодавства України, що встановлює відповідальність за злочини у сфері комп'ютерної інформації, на основі вивчення зарубіжних кримінальних законів і судової практики, а також міжнародно-правових документів, розроблених і прийнятих у цій галузі.

Аналіз окремих елементів злочинів, пов'язаних з використанням засобів комп'ютерної техніки розглядалися у працях А.А. Васильєва, О.Г. Волеводза, В.О. Мещерякова, В.О. Голубєва, Т.Л. Тропіної та інших науковців.

Проте, при розгляді особливостей протидії злочинам, пов'язаних із використанням засобів комп'ютерної техніки, недостатньо приділено уваги питанням міжнародної співпраці в оперативно-розшуковій діяльності, хоча стрімкий розвиток технологій практично стирає державні кордони для злочинців, дозволяючи їм одночасно здійснювати злочини в будь-якій країні світу. Метою статті є аналіз особливостей міжнародного співробітництва при розслідування кіберзлочинів.

Глобальна всесвітня мережа Internet, що об'єднала мільйони комп'ютерів, розташовані в різних країнах, і відкрила широкі можливості для отримання та обміну інформації, все частіше використовується в злочинних цілях. Поява електронних грошей і віртуальних банків, бірж, магазинів, за допомогою яких надаються реальні послуги в придбанні товарів, стало одним з факторів появи нового виду злочинів – «транснаціональних комп'ютерних злочинів». Сьогодні, разом із традиційною діяльністю, перед правоохоронними органами постало нове завдання попередження і розслідування злочинів у сфері використання комп'ютерних технологій – «кіберзлочинів».

Поняття кіберзлочину є поки незвичним для правоохоронних органів, проте злочинні дії, в яких використовується глобальна комп'ютерна мережа Internet, містять в собі велику суспільну небезпеку. Транснаціональний характер злочинності з використанням комп'ютерної мережі дає підстави вважати, що розробка спільної політики по основних питаннях повинна бути частиною будь-якої стратегії боротьби з кіберзлочинністю.Також певною мірою чинником, що сприяє зростанню цього нового виду злочинів, можна вважати відсутність належної взаємодії національних правоохоронних органів у питаннях попередження та розслідування таких видів злочинів.

Для врегулювання існуючих проблем на національному і міждержавному рівні виникла необхідність юридичного визначення в найбільш важливих правових нормах поведінки їх учасників, у боротьби з правопорушеннями, пов'язаними з використанням мережі Internet. Одним із серйозних кроків спрямованих на врегулювання цієї проблеми стало прийняття Радою Європи 23.11.2001 р. Конвенції по боротьбі з кіберзлочинністю [1]. Враховуючи складність проблеми, цей доку-

ISSN 1995-6134

мент став однією з перших міжнародних угод з юридичних і процедурних аспектів розслідування кіберзлочинів. Конвенцією по боротьбі з кіберзлочинністю передбачені скоординовані дії на національному та міждержавному рівнях щодо припинення несанкціонованого втручання в роботу комп'ютерних систем, незаконного перехоплення даних і втручання в комп'ютерні системи.

Підписання, державами, членами Ради Європи «Конвенції по боротьбі з кіберзлочинністю» («Конвенції»), стало результатом розуміння важливості проведення політики, спрямованої на захист суспільства від кіберзлочинів, необхідності прийняття відповідного законодавства та зміцнення міжнародного співробітництва. В Україні Конвенція була ратифікована у 2005 р. [2].

Однією з головних особливостей Конвенції є пропозиція виходити з того положення, що чільна роль у регулюванні кримінального процесу розслідування злочинів у сфері комп'ютерної злочинності належить національному законодавству. У силу цього Конвенція включає главу 2 «Заходи, які належить прийняти на національному рівні», в якій передбачено включення в національний кримінальний процес норм щодо процесуальних дій, специфічних для розслідування і судового розгляду справ про комп'ютерні злочини.

У коло процесуальних норм, пропонованих Конвенцією для включення в національне законодавство, входять слідчі дії, які доповнені рядом особливостей, пов'язаних зі специфікою, властивою доказовій інформації у формі комп'ютерних даних. Поряд з цим Конвенція передбачає необхідність формування на внутрішньодержавному рівні правових основ нових процесуальних дій.

До них віднесено, по-перше, негайне забезпечення збереженості отриманих комп'ютерних даних, включаючи дані про рух інформації, які були згенеровані і збережені за допомогою комп'ютерної системи, у разі якщо є підстави вважати, що ці дані можуть бути втрачені або модифіковані. Конкретний термін збереження не встановлений, але визначений як адекватний період часу, який дозволить компетентним органам домогтися розкриття цих комп'ютерних даних. Це означає, що пропонований процесуальний інститут не дає правових підстав для прямого доступу органів влади до комп'ютерної інформації, а лише створює умови для нього, будучи мірою попереднього характеру. При цьому під збереженням даних слід розуміти залишення їх у тому вигляді, в якому вони вже є в ЕОМ, захистивши від будь-яких зовнішніх впливів.

По-друге, негайне забезпечення збереження і часткове розкриття даних про рух інформації. Воно відрізняється від попереднього тим, що підлягає застосуванню у випадках, коли мова йде про необхідність збереження відомостей про повідомлення електрозв'язку, переданих по комп'ютерним мережам.

По-третє, видача розпорядження про пред'явлення. Таке розпорядження може бути віддано або особі, щодо надання комп'ютерних даних, які знаходяться під контролем цієї особи, або постачальнику послуг, щодо надання відомостей про його абонентів. До останніх віднесена будь-яка наявна у постачальника послуг інформація про користувачів, виражена як у формі комп'ютерних даних, так і в будь-який інший формі (за винятком даних про рух або змісті інформації), за допомогою якої можна встановити:

− тип використаного зв'язку, його технічні умови і час здійснення;

− особу користувача, його адресу, номера телефонів та інших засобів доступу;

− відомості про виставлені йому рахунки та здійснені ним платежі;

− будь-які інші відомості про місце встановлення комунікаційного обладнання.

Слід зазначити, що Конвенція допускає застосування даного виду нових повноважень виключно на індивідуальній основі для вирішення задач розслідування конкретних кримінальних справ. У зв'язку з цим потрібно розуміти, що ці повноваження не повинні використовуватися для того, щоб змусити всіх постачальників послуг постійно накопичувати і зберігати інформацію про своїх абонентів, а також всю передану ними комп'ютерну інформацію і т.д.

По-четверте, збір і запис із застосуванням технічних засобів у режимі реального часу даних про рух інформації, які передаються

ISSN 1995-6134

через комп'ютерні системи. Даний вид діяльності розрахований на застосування щодо відомостей про повідомлення, передані по мережах електрозв'язку, які створюються безпосередньо в момент реалізації таких повноважень. При цьому здійснюється передача нематеріальних об'єктів (наприклад, у формі електромагнітних імпульсів), а їх збір і запис не заважають проходженню самого повідомлення по мережах електрозв'язку до адресата.

По-п'яте, перехоплення даних про зміст повідомлень, переданих за допомогою комп'ютерних систем, здійснюваний як компетентними органами держави, так і постачальниками послуг за їх вказівкою. Даний інститут аналогічний попередньому, але стосується безпосередньо змістовної частини повідомлень, переданих по мережах електрозв'язку.

Хоча в Конвенції детально і не прописаний механізм правового регулювання реалізації двох останніх способів збирання комп'ютерної інформації, наявний досвід і співвідношення з нормами законодавства України та інших країн дозволяють стверджувати, що вони, найімовірніше, в даний час підлягають використанню шляхом проведення оперативно-розшукових заходів, передбачених пп.9 і 10 ст.8 Закону України «Про оперативно-розшукову діяльність» [3].

Варто зауважити, що оперативно-розшукова діяльність може здійснюватися тільки уповноваженими на те підрозділами державних органів (ст.5 вищевказаного Закону). У таких умовах безпосередня реалізація постачальниками послуг повноважень по збору і запису в режимі реального часу даних про рух інформації, перехопленню (збиранню і запису) даних про зміст повідомлень видається такою, що суперечить конституційним принципам законодавства.

Детальний виклад у Конвенції норм, що підлягають включенню в національне кримінально-процесуальне законодавство, створив необхідні умови для визначення в ній основних принципів міжнародного співробітництва її учасників. Загалом питанню співробітництва компетентних органів різних держав у боротьбі з комп'ютерними злочинами присвячена глава 3 Конвенції «Міжнародне співробітництво». В ній варто виділити декілька ключових аспектів.

При розслідуванні злочинів у сфері комп'ютерної інформації більшість запитів про взаємну правову допомогу стосуються питань, що так чи інакше зачіпають конституційні права громадян. У силу цього Конвенція виходить з того, що прийняття рішень за даними клопотаннями повинно перебувати у виключній компетенції одного-двох центральних органів, незалежно від підслідності та підвідомчості конкретних кримінальних справ (з урахуванням лише специфіки стадій слідства – попереднього і судового). Саме спеціально призначені центральні органи повинні підтримувати зв'язок безпосередньо один з одним. В Україні такими органами визначено Міністерство юстиції України (щодо запитів судів) та Генеральна прокуратура України (щодо запитів органів досудового слідства).

З урахуванням специфіки розслідування таких злочинів, Конвенцією передбачено доповнення загального порядку відносин при наданні взаємної правової допомоги. Так, в термінових обставинах допускається направлення запитів про взаємну правову допомогу з використанням оперативних засобів зв'язку, включаючи факсимільні повідомлення або електронну пошту, якщо такі засоби забезпечують відповідні рівні безпеки і підтвердження достовірності, з подальшим офіційним підтвердженням на вимогу запитуваної сторони. Згідно з пунктами «a» і «b» ч.9 ст.27 Конвенції запити про взаємну правову допомогу або пов'язані з ними повідомлення можуть надсилатися безпосередньо судовими органами сторін, а також через Інтерпол.

Поряд з цим Конвенцією пропонується введення раніше не врегульованого міжнародно-правовими документами порядку відносин – шляхом створення мережі щоденного цілодобового доступу (міжнародне позначення «24/7 Network», що може бути розшифровано як «доступ 24 години 7 діб на тиждень»).

В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для на-

ISSN 1995-6134

дання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. Серед ключових завдань контактних пунктів – забезпечення швидкого виконання функцій, передбачених Конвенцією, навіть якщо вони не відносять по національному законодавству до компетенції самого пункту.

Крім того, Конвенцією визначається можливість відправлення однієї з сторін інформації, отриманої в рамках її власного розслідування, якщо вона вважає, що розкриття такої інформації могло б допомогти стороні-одержувачу цих відомостей розпочати або проводити розслідування чи судовий розгляд відносно кримінальних злочинів.

Таким чином, 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.

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 і необхідні для розслідування. Це дає можливість правоохоронним органам проводити розслідування таких злочинів або вживати дії для збереження даних, які можуть бути знищені після закінчення певного моменту часу.

Безперечно, з правової точки зору велике значення мають і загальні принципи, що стосуються міжнародного співробітництва, які визначені в «Конвенції». Це питання видачі комп'ютерних злочинців і надання один одному широкої взаємодопомоги для розслідування кримінальних справ, пов'язаних з комп'ютерними системами і даними, так само як і для збору електронних доказів.

ЛІТЕРАТУРА

1. Conventionon Cybercrime / Councilof Europe [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm. – 2001.

2. Закон України «Про ратифікацію Конвенції про кіберзлочинність» // ВВР України. – 2006. – № 5. – Ст. 71.

3. Закон України «Про оперативно-розшукову діяльність» // ВВР України. – 1992. – № 22. – Ст. 303.

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

Розглянуто особливості транснаціональних кіберзлочинів та труднощі, які виникають при їх розслідуванні. Також проаналізовано ключові положення Конвенції по боротьбі з кіберзлочинністю, як основного документу, що регулює питання міжнародного співробітництва в цій сфері.

***

Бабакин В.Н. Особенности международного сотрудничества при расследовании киберпреступлений

Рассмотрены особенности транснациональных киберпреступлений и трудности, которые возникают при их расследовании. Также проанализированы ключевые положения Конвенции по борьбе с киберпреступностью, как основного документа, регулирующего вопросы международного сотрудничества в этой сфере.

***

Babakin V.N. International Cooperation Singularities at Fact-finding of Cybercrimes

The features of transnational cyber crimes and the difficulties encountered in their investigation are made. Also the key provisions of the Convention on the fight against cybercrime, as the main document that regulates international cooperation in this area analyzed.