РОЗДІЛ VII. КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 351.74: 061.1: 343.451(100)

СПІВРОБІТНИЦТВО ТА ВЗАЄМОДІЯ ПРАВООХОРОННИХ ОРГАНІВ РІЗНИХ ДЕРЖАВ СВІТУ В БОРОТЬБІ З МІЖНАРОДНОЮ КІБЕРЗЛОЧИННІСТЮ

Сабадаш В.П., к.ю.н., доцент

Запорізький національний університет

У статті розглянуто питання взаємодії та співробітництва правоохоронних органів різних держав світу в боротьбі з міжнародною кіберзлочинністю.

Ключові слова: співробітництво, взаємодія, злочин, кіберзлочинність, правоохоронні органи.

Сабадаш В.П. СОТРУДНИЧЕСТВО И ВЗАИМОДЕЙСТВИЕ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ РАЗЛИЧНЫХ ГОСУДАРСТВ МИРА В БОРЬБЕ С МЕЖДУНАРОДНОЙ КИБЕРПРЕСТУПНОСТЬЮ / Запорожский национальный университет, Украина

В статье рассмотрены вопросы взаимодействия и сотрудничества правоохранительных органов различных государств мира в борьбе с международной киберпреступностью.

Ключевые слова: сотрудничество, взаимодействие, преступление, киберпреступность, правоохранительные органы.

Sabadash V.P. COOPERATION AND INTERACTION OF LAW ENFORCEMENT BODIES OF THE VARIOUS STATES OF THE WORLD IN STRUGGLE AGAINST THE INTERNATIONAL CYBERCRIMINALITY / Zaporizhzhya national university, Ukraine

In article questions of interaction and cooperation of law enforcement bodies of the various states of the world in struggle against the international cybercriminality are considered

Key words: cooperation, interaction, crime, cybercriminality, law enforcement bodies.

В умовах інтенсивного впровадження передових інформаційно-телекомунікаційних технологій в усі сфери діяльності світового співтовариства, об'єднанням інформаційних ресурсів у єдину глобальну інформаційну інфраструктуру однією з важливих умов економічного процвітання й духовного розвитку держав є інтеграція у світове інформаційне співтовариство.

Однак входження в інформаційне співтовариство окремих держав не скасовує наявності в них національних інтересів і необхідність забезпечення їхньої безпеки. Крім того, широке використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому висуває вирішення проблем інформаційної безпеки в число основних. Крім прямого збитку від можливих фактів несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися в засіб придушення волі людини, стати джерелом серйозної загрози державності й духовного життя особистості.

Актуальність теми статті обумовлена тим, що зростання науково-технічного прогресу обумовлює не тільки прогресивні зміни в економіці, але й негативні тенденції розвитку злочинного світу, призводить до появи нових форм і видів злочинних зазіхань. Це проявляється в тому, що злочинні групи активно використовують у своїй діяльності новітні досягнення науки й техніки, застосовують усілякі комп'ютерні пристрої та нові інформаційно-обробні технології.

Крім того, у сфері зближення підходів з питань протистояння сучасним погрозам в інформаційній сфері продовжує залишатися актуальною тема розвитку саме прозорої та оперативної взаємодії правоохоронних підрозділів різних країн світу. Надто важливо

нарощувати обсяги й темпи обміну інформацією про функціонування трансграничних злочинних груп в Інтернет – просторі, про злочинні організації та особи, що використовують інформаційні технології в терористичних цілях, про нові методи й способи скоєння злочинів.

Вивчення стану наукової розробленості проблем співробітництва та взаємодії правоохоронних органів різних держав у боротьбі з міжнародною кіберзлочинністю показало, що на сучасному етапі спеціального дослідження із цих проблем не проводилося. Проте необхідно зазначити, що окремі аспекти взаємодії й співробітництва розглядалися в роботах Ю.М. Батурина, П.Д. Біленчука, М.С. Вертузаєва, В.Б. Вєхова, В.О. Голубєва, М.Д. Дихтяренко, Є.І. Панфілової, О.М. Попова, Н.А. Селіванова та ін.

Метою даної статті є комплексне вивчення проблем, пов'язаних із питаннями співробітництва та взаємодії правоохоронних органів різних держав світу в боротьбі з міжнародною кіберзлочинністю, та на базі цього розробка пропозицій, спрямованих на підвищення ефективності кримінально-правового регулювання боротьби з даним видом злочинного зазіхання.

Із впровадженням у повсякденне життя суспільства й держави передових інформаційних технологій, зростає вплив інформаційних погроз на інформаційно-телекомунікаційні системи, інформаційні ресурси державних органів і комерційних структур з боку кримінального світу та окремих осіб, з метою скоєння протиправних дій.

Аналіз статистичних даних дозволяє судити про наявні тенденції в цій сфері. Так, за даними МВС РФ, у 2007 році в Російській Федерації було зареєстровано 7236 злочинів у сфері комп'ютерної інформації [1], у 2008 році – 9010 злочинів (+ 24, 5%) [2], а у 2009 році – 11636 злочинів, що на 29, 1 % більше ніж за 2008 рік [3]. В Україні, за даними МВС України, у 2007 році зареєстровано 656 злочинів у сфері високих технологій, у 2008 році – 691 злочин (+ 5,3%) [4], а у 2009 році зареєстровано 707 злочинів у сфері високих технологій, що на 2,3 % більше, ніж за 2008 рік [5].

Половина зафіксованих комп'ютерних злочинів у світі відноситься до несанкціонованого доступу до комп'ютерної інформації. Останнім часом ми можемо спостерігати зростання кількості злочинів, що вчиняються групами, зростання кількості трансграничних комп'ютерних злочинів. Крім того, зростає корислива спрямованість комп'ютерних злочинів разом із нанесеним матеріальним збитком.

Як і раніше, високою залишається латентність комп'ютерної злочинності, неможливим стає одержання повної картини комп'ютерної злочинності, яке викликано тим, що і державні і комерційні структури, які піддавалися комп'ютерним злочинам, усіляко намагаються сховати такі факти, боячись втратити авторитет, не схильні афішувати нанесений збиток і слабку систему захисту інформації.

Усе більше ми бачимо, як комп'ютерні злочини стають лише першим кроком у ланцюжку кримінальних діянь, спрямованих на інші, традиційні злочини – розкрадання, вимагання, шахрайство й т.п. Останнім часом у воєнних діях збройних сил різних держав простежується тенденція масового застосування методів комп'ютерного підриву. При цьому інша держава буде теж протистояти комп'ютерному підриву, буде застосовувати більш витончені методи боротьби. Результатом цього всього може стати поява глобальних "інформаційних війн". З кожним днем злочини стають більше витонченими та такими, що наносять величезний економічний і політичний збиток практично всім країнам світу.

На жаль, чекати значного зниження кількості комп'ютерних злочинів не доводиться. З огляду на загальну тенденцію до конвергенції мереж і гіперпідключеності галузі, число порушень у сфері комп'ютерної безпеки рік у рік буде зростати. Генеральний директор IBM у Східній Європі й Азії Кирило Корнильєв у рамках десятого, ювілейного "Інфофоруму" відзначив, що, чим більше компонентів буде містити мережа, тим більше погроз безпеки буде вона мати [6].

Однією із серйозних причин складності розслідування комп'ютерних злочинів є їх транснаціональний характер, коли зловмисник може перебувати в будь-якій країні світу й здійснювати протиправні дії відносно будь-якої держави або комерційної структури. Тому для успішного розслідування, збору доказів та притягнення зловмисників до відповідальності за злочини, пов'язані з використанням комп'ютерів, виникає необхідність відстеження злочинної

діяльності та її наслідків через ланцюжок проксі-серверів, анонімайзерів та інших служб Інтернету, що нерідко перебувають у різних державах.

Крім того, не є секретом, що членами злочинних груп можуть бути громадяни різних держав світу, що, у свою чергу, викликає складності в проведенні процесуальних дій та зборі доказів. Тому й у розслідуваннях застосовуються нові методи в сполученні із класичними. Саме це сполучення і є головною умовою будь-якого успішного розслідування.

У ході боротьби зі злочинами в сфері інформаційних технологій виникають численні проблеми правового характеру, викликані нематеріальністю й часом недовговічністю електронних доказів. Складність вирішення проблем, характерних для кіберзлочинності, робить особливо актуальним міжнародне співробітництво, для чого країни повинні, в остаточному підсумку, мати у своєму розпорядженні відповідні та суміжні між собою правові, процесуальні та нормативні засоби.

Вивчення практики розслідування комп'ютерних злочинів призводить до необхідності налагодження взаємодії між правоохоронними органами різних держав світу. Однак, говорячи про міжнародне співробітництво в даній області, доводиться констатувати, що кроки, які вживаються в цій області, носять недостатній характер і не одержують належного розвитку в конкретних двосторонніх і багатобічних проектах у сфері інформатизації та захисту інформації.

Слід мати на увазі, що для вирішення проблеми кіберзлочинності необхідний всебічний підхід. Безумовно, одним із кроків у виробленні єдиних підходів до заходів протидії комп'ютерним злочинам, стало набрання чинності міжнародною Конвенцією по боротьбі з кіберзлочинністю, яка була прийнята в рамках Ради Європи 23 листопада 2001 року та ратифікована Україною у вересні 2005 року. Дана Конвенція стала першою міжнародною угодою з юридичних і процедурних аспектів розслідування та кримінального переслідування кіберзлочинів, у якій передбачаються скоординовані на національному й міждержавному рівнях дії, спрямовані на недопущення несанкціонованого втручання в роботу комп'ютерних систем.

Окремий розділ Конвенції присвячений міжнародному співробітництву з наступних питань: екстрадиції у зв'язку з кримінальними правопорушеннями; добровільного надання інформації щодо проведення розслідування або переслідування кримінальних злочинів; процедур, пов'язаних із запитами про взаємну допомогу у випадку відсутності міжнародних угод між країнами. Також у документі описані проблеми взаємодії правоохоронних органів у випадках, коли кіберзлочинець та його жертва перебувають у різних країнах і підкоряються різним законам.

У конвенції висвітлюються питання зберігання особистої інформації клієнтів інтернет-провайдерів на випадок, якщо це буде потрібно при розслідуванні кіберзлочинів [7].

Крім вищевказаної Конвенції, багато країн світу, у тому числі й Україна, беруть участь у процесах пошуку загальних рішень і їхньої погодженої реалізації, які розвиваються в рамках ООН, ЮНЕСКО, Європейського Союзу, Співдружності незалежних держав (СНД), Шанхайської організації співробітництва, ЕВРАЗЭС та інших організацій.

Існує ряд двосторонніх угод, створюються об'єднані робочі групи правоохоронних органів різних держав світу з питань взаємодії та співробітництва в даній сфері. Існує у світі також практика проведення спільних заходів при розслідуванні комп'ютерних злочинів. Спільні операції проводяться в рамках боротьби з дитячою порнографією, шахрайських дій у мережі Інтернет, міжнародним тероризмом тощо.

Однак на проблему ефективності співробітництва і взаємодії правоохоронних органів різних країн світу впливають також існуючі в наш час механізми такого міжнародного співробітництва, які не сприяють повному й швидкому одержанню з іноземної держави доказів у формі комп'ютерних даних. На думку О.Г. Волеводза, причини тому наступні:

По-перше, традиційні форми співробітництва держав в області правової допомоги по кримінальних справах передбачають направлення письмових клопотань (прохань) про надання правової допомоги. Це вимагає певного часу для їхнього пересилання, виконання та одержання письмових матеріалів, що для розслідування такої категорії злочинів означає втрату доказової інформації.

По-друге, заходи, навіть якщо вони швидко використовуються в рамках взаємної правової допомоги, у кращому разі дозволяють виявити, закріпити й вилучити лише інформаційні сліди, що перебувають на серверах і розташовані на території певної держави (наприклад, країни місцезнаходження потерпілого або країни перебування особи, що скоїла комп'ютерний злочин). Коли ж комп'ютерне повідомлення по телекомунікаційних каналах проходить через третю (четверту, п'яту) країну, надання правової допомоги може тривати нескінченно довго. І чим більше країн, через які посилається повідомлення, тим вище ймовірність того, що правоохоронним органам не вдасться з використанням традиційних форм взаємної правової допомоги організувати належну роботу з розслідування таких злочинів.

По-третє, у рамках більшості діючих нині міжнародних договорів з питань взаємної правової допомоги в кримінальному процесі, можливість її надання у формах, що обмежують права громадян, визначається принципом "подвійного визначення складу злочину", відповідно до якого держава не може співробітничати з іншою щодо розслідування та судового переслідування діянь, які не криміналізовані в запитуваній державі. Як справедливо відзначають Є.І. Панфілова та О.М. Попов, різниця у визначеннях різних складів злочинів у різних країнах досить істотна. Це дозволяє особам, що вчиняють злочини у сфері комп'ютерної інформації, вибирати для сеансів зв'язку ті країни, де аналогічні діяння не є криміналізованими [8, 23].

По-четверте, на ринку інформаційних послуг дуже часто діють транснаціональні компанії, які надають послуги (наприклад, у Європі), але зберігають всі дані про такі послуги у головному офісі, розташованому на іншому континенті [9].

На нашу думку, для успішної боротьби з кіберзлочинністю обов'язковими є три складові:

- гармонізація національного законодавства щодо боротьби із комп'ютерною злочинністю за вимогами міжнародного права;
- висока професійна підготовка правоохоронних органів – від слідчого до всієї судової системи;
- співробітництво та правовий механізм по взаємодії правоохоронних органів різних держав світу.

Для найбільш ефективного співробітництва та взаємодії правоохоронних органів різних країн світу в боротьбі з міжнародною кіберзлочинністю необхідне удосконалення національних правових механізмів, що забезпечують здійснення обміну оперативною інформацією із правоохоронними органами різних країн. Є сенс розглянути можливість розробки системи захисту інформації, що передається по каналах міжнародної мережі національних контактних пунктів, при цьому можуть застосовуватися засоби криптографії, створення захищених віртуальних мереж, особливі методи ідентифікації й багато чого іншого. Корисним бачиться впровадження в практику їхньої роботи пропозиції щодо затвердження типових формалізованих документів інформаційного обміну і розробки словника умовних кодів виявлених кіберзлочинів, формування переліку видів трансграничних злочинів, фактів прояву тероризму й екстремізму, шахрайських схем і фактів хакерських нападів, щодо яких інформація негайно повинна направлятися правоохоронним органам потерпілої сторони по каналах мережі національних контактних пунктів.

Крім того, необхідним вбачається подальший розвиток співробітництва в області забезпечення інформаційної безпеки, та проведення заходів щодо її захисту, переважно на основі двосторонніх і багатосторонніх договорів. Успішне вирішення проблем інформаційної безпеки, на наш погляд, можливе лише при ефективній взаємодії державних структур різних держав, тим більше, що необхідна правова база вже є. Є саме через те, що в наш час між багатьма державами світу вже укладено ряд як двосторонніх, так і багатосторонніх угод в області захисту інформації.

Таким чином, провівши дослідження щодо співробітництва та взаємодії правоохоронних органів різних держав світу у боротьбі з міжнародною кіберзлочинністю, можемо зазначити, що співробітництво уявляється доцільним здійснювати за наступними напрямками:

1) Гармонізації національних законодавств у сфері інформаційної безпеки, у тому числі протидії іноземним технічним розвідкам;

2) Організації спільних виробництв засобів захисту інформації;

3) Підготовки та перепідготовки фахівців із профільних напрямків;

4) Розвитку інноваційної діяльності.

ЛІТЕРАТУРА

1. Состояние преступности в Российской Федерации за 2007 год // [Электронный ресурс]. – Режим доступа: http://www.mvd.ru/files/u281KzbmtHplrXo.pdf.
2. Состояние преступности в Российской Федерации за 2008 год // [Электронный ресурс]. – Режим доступа: http://www.mvd.ru/files/PUeh34ZSL9gjacp.pdf.
3. Состояние преступности в Российской Федерации за 2009 год // [Электронный ресурс]. – Режим доступа: http://www.mvd.ru/files/AauTOcPxyhbg2fK.pdf.
4. Стан та структура злочинності в Україні (2007-2008 р.р.) // [Електронний ресурс]. – Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/170319.
5. Стан та структура злочинності в Україні (2008-2009 р.р.) // [Електронний ресурс]. – Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/233004.
6. Чем ответит Россия на киберугрозы ? // [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/newstext.php?news_id=41255.
7. Конвенція про кіберзлочинність // [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575.
8. Панфилова Е.И. Компьютерные преступления: Серия "Современные стандарты в уголовном праве и уголовном процессе" / Е.И. Панфилова, А.Н. Попов; Науч. ред. проф. Б.В. Волженкин. – СПб.: Изд-во С.-Петербург. юрид. ин-та Генеральной прокуратуры РФ, 1998. – 48 с.
9. Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. – М.: ЮИ МВД РФ, 2003. – 245 с.

УДК 35.078.3 : 343.451 : 044 (477) (075.8)

ВИСОКОТЕХНОЛОГІЧНИЙ ПРОФЕСІОНАЛІЗМ ПРОКУРОРА-КРИМІНАЛІСТА

Синєокий О.В., к.ю.н., доцент

Запорізький національний університет

Узунов П.П., експерт

Науково-дослідний експертно-криміналістичний центр при ГУ МВС України в Запорізькій області

У статті авторами проаналізовані і науково обґрунтовані теоретико-методологічні засади розвитку психолого-акмеологічної концепції професійної діяльності прокурора-криміналіста. На підставі проведеного дослідження авторами визначаються шляхи та перспективи акмеологічних розвідок теоретичної моделі професіоналізму особистості прокурора-криміналіста в сучасних умовах реформування системи органів прокуратури України.

Ключові слова: акмеологія; професійна діяльність; професіоналізм; прокурор-криміналіст.

Синеокий О.В., Узунов П.П. ВЫСОКОТЕХНОЛОГИЧЕСКИЙ ПРОФЕССИОНАЛИЗМ ПРОКУРОРА-КРИМИНАЛИСТА / Запорожский национальный университет, Научно-исследовательский экспертно-криминалистический центр при ГУ МВД Украины в Запорожской области, Украина