ність експертів. Судження спеціаліста і експерта вбирається в форму його укладення, також може бути проведено допит спеціаліста або експерта. Перевірка інформації з мережі Інтернет може здійснюватися шляхом отримання нових доказів (наприклад, висновок експерта, допит потерпілого), а також шляхом їх зіставлення.

Таким чином, загальний алгоритм пошуку криміналістично значущої інформації в мережі Інтернет уявляється етапним та складається з взаємообумовлених дій, що ґрунтуються на інформаційно-комунікаційному та техніко-технологічному підходах.

Ключові слова: джерело інформації, криміналістична інформація, аналітична робота, кіберпростір, мережа Інтернет.

Ключевые слова: источник информации, криминалистическая информация, аналитическая работа, киберпространство, сеть Интернет.

Key words: source of information, criminalistics information, analytical work, cyberspace, Internet network.

СТАУРСЬКА ОЛЕКСАНДРА МИКОЛАЇВНА

Національний університет «Одеська юридична академія»,
аспірант кафедри криміналістики

ПРОБЛЕМИ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ У КОНТЕКСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

На сьогоднішній день, проблема боротьби із кіберзлочинністю набуває все більш великих масштабів. Законодавче регулювання даної проблеми на міжнародному рівні розглядається багатьма вченими. Впровадження комп'ютерних технологій у різноманітні сфери життя українського суспільства відкриває широкі перспективи його соціально-економічного і духовного розвитку. Але разом із цим результати науково-технічного прогресу створюють нові можливості для вчинення різноманітних злочинів.

Аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності. Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж.

Основна проблема боротьби зі злочинністю в мережі Інтернет полягає в транснаціональності самої мережі і у відсутності механізмів контролю, необхідних для правозастосування. Коли мережа Інтернет створювалася технологічно як структура без ієрархії і без якогось «ядра», зруйнувавши які, можна було б паралізувати її роботу, навряд чи хтось міг уявити масштаби розвитку проекту,

спочатку не призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, і навряд чи хтось міг передбачити подальший масштаб її розвитку та її соціальну та економічну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини укупі з її доступністю і легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі і відсутність національних кордонів у кіберпросторі зумовили можливості для зростання злочинності та на роки відклали розробку механізмів соціального та правового контролю у сфері використання інформаційних мереж для вчинення злочинів.

В останні роки інформаційні мережі розвиваються занадто швидко, щоб існуючі механізми контролю встигали реагувати на нові проблеми. Хмарна обробка даних, автоматизація атак, вразливість персональної інформації в соціальних мережах: поширення так званої «інформаційної зброї», прикладом якого є вірус Stuxnet, розроблений, на думку фахівців, для атак на ядерну промисловість Ірану, але при цьому заподіяв чималої шкоди інфраструктурі багатьох інших країн – на всі ці проблеми правове регулювання поки не може знайти відповіді [1].

З того моменту, держава включається в інформаційний обмін за допомогою мережі Інтернет, вона сама та її громадяни стають вразливими для посягань з точки земної кулі. Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно. Наприклад, як показує приклад атак на ядерне виробництво Ірану, навіть відключення особливо важливих для держави об'єктів від глобальних інформаційних мереж не захищає їх від можливих атак: вірус Stuxnet, поширювався через портативні накопичувальні пристрої, що підключаються до комп'ютера через порт USB. Єдиний спосіб повністю убезпечити особливо важливі об'єкти для функціонування суспільства – це повністю відключити мережу Інтернет не тільки від об'єктів захисту, а й у всій державі в цілому. Зрозуміло, це неможливо, оскільки інформаційні технології відіграють найважливішу роль у функціонуванні суспільства.

Кількість користувачів. Із збільшенням числа користувачів зростають, такі фактори ризику: збільшується залежність суспільства від інформаційних технологій, що, у свою чергу, обумовлює його вразливість до різного роду інформаційних зазіхань; збільшується можливість використання мережі для вчинення злочинів, а також росте потенційна можливість стати жертвою використання інформаційних технологій в злочинних цілях. При цьому вчинення злочину не вимагає великих зусиль і витрат – достатньо мати комп'ютер, програмне забезпечення та підключення до інформаційної мережі. Не потрібно навіть глибоких технічних знань: існують спеціальні форуми, на яких можна придбати програмне забезпечення для вчинення злочинів, вкрадені номери кредитних карт і ідентифіка-

ційні дані користувачів, а також скористатися послугами з допомоги в здійсненні електронних розкрадань і атак на комп'ютерні системи як в цілому, так і на окремих стадіях вчинення злочинів [2].

Автоматизація та швидкість використання. Комп'ютерні дані можуть бути передані з однієї точки світу в іншу за кілька секунд. Більше того, практично будь-яка передача даних у мережі зазвичай включає декілька країн, оскільки, коли інформація розбивається на частини і йде по найбільш зручним та доступним каналам. Контролювати передачу даних, з урахуванням їх обсягу та кількості користувачів, дуже важко, якщо не неможливо. Злочинець, потерпілий, сервер з необхідною інформацією можуть перебувати в різних країнах і на різних континентах, що вимагає співпраці правоохоронних органів декількох країн при розслідуванні злочину.

Анонімність мережі Інтернет, вразливість бездротового доступу і використання проксі-серверів істотно ускладнюють виявлення злочинців: для вчинення злочину може використовуватися «ланцюжок» серверів, злочини можуть бути вчинені шляхом виходу в Інтернет через точки загального доступу, такі, як Інтернет-кафе, технології дозволяють також «зламати» доступ в чужу бездротову мережу Wi-Fi. Таким чином, існує достатньо способів ускладнити розслідування злочинів.

Проблема територіальної юрисдикції в кіберпросторі та правового співробітництва. Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп'ютерних даних, які дуже вразливі за своєю природою і можуть бути швидко знищені. У цій ситуації традиційні механізми правової взаємодопомоги і принцип суверенітету, одним з проявів якого є те, що тільки правоохоронні органи держави можуть проводити слідчі дії на його території, вимагають безліч формальних погоджень, роблячи розслідування транснаціональних кіберзлочинів проблематичним. Окрім співробітництва правоохоронних органів, яке вимагає тимчасових витрат і дотримання безлічі формальностей, встає також питання про дотримання фундаментального принципу nullum crimen, nulla poena sine lege, коли необхідна подвійна криміналізація діяння: як у країні, з території якої діяв правопорушник, так і в державі, де знаходиться потерпілий. Різниця у криміналізації діянь, відмінності у визначенні тяжкості вчиненого діяння, особливо в сфері релігійних злочинів і злочинів проти громадського порядку, в області нелегального контенту, в екстремістських злочинів значно ускладнюють процес співробітництва правоохоронних органів, іноді роблячи його неможливим [3].

Таким чином, ефективний контроль негативних явищ у кібепросторі, таких як злочинність, вимагає набагато більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності. Саме тому окрім гармонізації кримінально-правових норм потрібна гармонізація процесуальних інструментів і вироблення нових механізмів міжнародного

співробітництва. Важливу роль у боротьбі з кіберзлочинністю тому грають міжнародні угоди у відповідній області, такі, як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) та ін. [4].

Всі зазначені інструменти не є за своєю суттю універсальними міжнародними інструментами, незважаючи на те, що такі угоди, як Конвенція Ради Європи, вийшли за своїм впливом далеко за рамки регіону, в якому вони були прийняті. Однак світова спільнота поки не володіє ні міжнародним органом, який спеціально займається інтернет-злочинністю, ні загальносвітовим правовим інструментом, що визначає масштаби відповідальності за відповідні злочини, і, що більш важливо – принципи співробітництва при розслідуванні протиправних діянь.

Однак, оскільки жодна держава не може захистити себе, вживаючи заходів тільки на національному рівні, для комплексної протидії кіберзлочинності необхідні:

– залучення спеціалістів до роботи з питаннями, що стосуються кіберпростору

– механізм вирішення юрисдикційних питань у кіберпросторі.

– гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;

– налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні.

Процес вироблення заходів на міжнародному рівні, як показує досвід, сам по собі є комплексною проблемою. Однак це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати і переслідувати кіберзлочини.

Таким чином міжнародне співробітництво є ключовим моментом у ліквідації правового застою, існуючого між розвитком інформаційних технологій та реагуванням на ці технології законодавства.

Список використаної літератури:

1. Біблійна Естер і кіберверсія війни з Іраном [Електронний ресурс] – 2010. – 10 жовтня. – Режим доступу: http://txt.newsru.ua/press/01oct2010/cyber.html.
2. Киберпреступность набирает обороты с развитием безналичных платежей [Электронный ресурс] // Экономическая аналитика. – 2013. – 17 мая. – Режим доступа: http://ea.vuk.com.ua/2013/05/17/киберпреступность–набирает–обороты.
3. Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста. – № 5. – 2013. – С. 148–160.

4. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби / Н. В. Савчук // Теоретичні та прикладні питання економіки: зб. наук. праць. – К.: Видавничо–поліграфічний центр «Київський університет», 2009. – Вип. 19. – С. 338–342.

Ключові слова: розслідування, кіберпростір, мережа Інтернет, транснаціональна злочинність.
Ключевые слова: расследование, киберпространство, сеть Интернет, транснациональная преступность.
Key words: investigation, cyberspace, Internet network, transnational crime.

ТОЛПИГО ДЕНИС МИКОЛАЙОВИЧ

Національний університет «Одеська юридична академія»,
здобувач кафедри криміналістики,
прокурор Одеської місцевої прокуратури № 1, юрист 1 класу

ПРАКТИЧНІ АСПЕКТИ ВИЗНАЧЕННЯ ДОПУСТИМОСТІ ДАНИХ, ОТРИМАНИХ В ХОДІ ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ТА НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Чинний Кримінальний процесуальний кодекс України передбачає можливість проведення як оперативно-розшукових заходів (ОРЗ), так і негласних слідчих (розшукових) дій при проведенні досудового розслідування кримінальних проваджень. Однак постає основне питання допустимості доказів, отриманих в ході проведення ОРД (ОРЗ) та НСРД в доказуванні по кримінальному провадженню. НСРД та ОРД (ОРЗ) мають низку процесуальних відмінностей, до яких, наприклад, можна віднести певну відмінність підстав проведення.

Так, на думку С.І. Ніколаюка [1], фактичними підставами проведення НСРД визначаються такі: наявність інформації про злочини, що готуються або вчинені невстановленими особами; наявність інформації про осіб, які готують або вчинили злочини; наявність інформації про осіб, які переховуються від органів розслідування або ухиляються від відбування кримінальної відповідальності. В свою чергу, ст. 6 Закону України «Про оперативно-розшукову діяльність» визначає наступні підстави проведення відповідних дій:

1) наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, про:

– злочини, що готуються;

– осіб, які готують вчинення злочину;