УДК 342.721

А.М. НОВИЦЬКИЙ, *кандидат юридичних наук (Ph.D), старший науковий співробітник,*
начальник відділу дослідження проблем протидії
податковим правопорушенням НДЦ з проблем оподаткування
Національного університету ДПС України

ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ В ІНТЕРНЕТ: ПРОБЛЕМИ ПРАВОЗАСТОСУВАННЯ

Анотація. *Щодо проблемних питань правового забезпечення проведення оперативно-розшукових заходів у мережі Інтернет.*

Створення мережі Інтернет стало одним з важливих етапів визнання переходу людства до інформаційного суспільства. Суспільство знань, інформаційне суспільство, постіндустріальне суспільство – декілька критеріїв оцінки та визначення. Проте сутність одна – базисом нових суспільних відносин виступає інформація. Боротьба за інформацію, володіння та маніпуляція нею стали одним із досить впливових елементів, що часто призводить до деліктних правовідносин. Тому Інтернет, який досить активно розвивається, стає інструментом для здійснення правопорушень в інформаційній сфері.

Протидія деліктним відносинам, встановлення належного державного впливу на негативні елементи, створення належної системи протидії злочинам у мережі Інтернет – це новий напрям протидії правопорушенням.

Проблеми боротьби із злочинами у сфері високих технологій, в мережі та із застосуванням Інтернету все більше привертають увагу вітчизняних науковців: В.М. Брижка, Р.А. Калюжного, В.А. Некрасова, В.Я. Мацюка, І.Ф. Хараберюша, В.С. Цимбалюка, М.Я. Швеця та зарубіжних: Ю.М. Батуріна, В.Б. Вехова, А.Н. Караханьяна, В.В. Крилова, В.А. Мінаєва, І.А. Наумова, А.З. Овчинського, А.Р. Серго, Б.Х. Толеубекова, В.Н. Черкасова та ін. Аналіз публікацій в сфері інформатизації оперативно розшукової діяльності, здійснення її із застосуванням новітніх інформаційних технологій не дає можливості говорити про розробку цілісної програми супроводу оперативно-розшукової діяльності (далі – ОРД) в Інтернеті. Більше того, практично відсутні публікації щодо можливості та тактики проведення спеціальних заходів оперативними підрозділами в мережі. Саме тому основною метою даної публікації ми вбачаємо необхідність розглянути можливі елементи втручання держави через спеціально уповноважені органи, в управління суспільними відносинами та встановлення належного контролю за протиправною діяльністю в мережі Інтернет.

Міжнародна практика та досвід боротьби зі злочинністю свідчать, з одного боку, про появу і широке поширення злочинів у сфері нових інформаційних технологій, а з іншого, – про збільшення ролі нових методів отримання доказів і перспективності використання технологій у цій діяльності [1].

Розглянемо один із прикладів, коли лише за допомогою оперативно-розшукових заходів у мережі Інтернет можливо встановити злочинні дії особи.

Ніхто ще не відміняв статті 208 Кримінального кодексу України, де передбачена відповідальність за незаконне відкриття або використання за межами України валютних рахунків. Зокрема, в даній статті зазначено, що незаконне, з порушенням встановленого законом порядку, відкриття або використання за межами України валютних рахунків

© А.М. Новицький, 2009

фізичних осіб, вчинене громадянином України, що постійно проживає на її території, а так само валютних рахунків юридичних осіб, що діють на території України, вчинене службовою особою підприємства, установи чи організації або за її дорученням іншою особою, а також вчинення зазначених дій особою, яка здійснює підприємницьку діяльність без створення юридичної особи.

Виникає досить колізійна ситуація, коли користувачі Інтернету відкривають валютні рахунки у “віртуальних банках”, існування яких передбачене законодавствами окремих держав світу (наприклад, Сінгапур). Постають запитання: чи будуть злочином дії по відкриттю та використанню рахунків фізичними та юридичними особами України в таких банківських установах, як проконтролювати ці банківські операції, як на законних підставах зробити запит до банківської установи?

Крім того, послугами таких банківських установ, які здійснюють свою діяльність лише у віртуальному світі Інтернеті, все більше користуються активні користувачі мережі. Це не тільки операції з оплати за товари та послуги, це і накопичення коштів на рахунках і відкриття депозитних рахунків, і навіть операції з кредитування. Постає запитання: чи порушуються правила відкриття рахунків, які встановлені в Україні, при відкритті та використанні рахунків в Інтернет-банках? З одного боку, чинним національним законодавством не передбачено заборону або спеціальні правила щодо відкриття та використання валютних рахунків в Інтернет-банках. Проте, з іншого боку, встановлена чітка процедура отримання дозволу Нацбанку для відкриття валютного рахунку за межами держави. Тобто використання таких рахунків уже є злочином за національним кримінальним законодавством.

Отримати інформацію про відкриття та використання рахунків у Інтернет-банках практично неможливо. Перш за все, це зумовлено тим, що вони не знаходяться в межах національної юрисдикції і тому не зобов’язані надавати відповіді на запити відповідних контролюючих та правоохоронних органів нашої держави більше того, інформація про клієнтів банку та про банківські операції в усьому світі вважається таємницею.

Як же встановити факт правопорушення та притягнути винних осіб до відповідальності? Очевидно, тут необхідно застосування оперативно-розшукових заходів у мережі Інтернет з використанням спеціальної техніки, спеціальних програм та відповідної підготовки суб’єктів проведення таких оперативно-розшукових заходів. Зокрема, А.С. Овчинський відмічав, що із застосуванням спеціальних технічних засобів і комп’ютерних технологій для добування, обробки та аналізу оперативно-розшукової інформації в останні роки в розвитку ОРД намітились нові напрями [3].

Тактика проведення спеціальних оперативних заходів із встановлення злочинної діяльності повинна визначатись у кожному конкретному випадку та залежати від наявної інформації, яка дає право на проведення ОРД, та можливостей спецпідрозділів, які будуть здійснювати відповідні заходи.

Необхідно відмітити, що проведення оперативно-розшукових заходів у мережі Інтернет – це досить складна система, яка передбачає наявність специфічної (матеріально-технічної, комп’ютерної, програмної, телекомунікаційної) підготовки. Особи, яким буде поставлено конкретне оперативно-розшукове завдання, повинні мати спеціальну підготовку, володіти матеріальною базою ОРД в Інтернеті та вміти проводити такі операції.

Очевидно, необхідно говорити про необхідність створення спеціального підрозділу в одному із правоохоронних органів, який би систематизовано, з відповідною спеціальною підготовкою та з можливістю застосування найновішої техніки міг би здійснювати оперативно-розшукові заходи в мережі Інтернет. Про доцільність широкого

впровадження даної ідеї в усіх правоохоронних органах говорити ще рано, перш за все через значні матеріальні затрати, для забезпечення роботи такого підрозділу та, що дуже важливо, відсутність належного правового механізму здійснення таких оперативних заходів у мережі Інтернет.

Відзначаючи необхідність створення спеціалізованих органів, які б займались оперативно-розшуковою роботою в мережі, відмітимо, що на сьогодні вже розроблено значний інструмент для здійснення таких заходів. Поряд із загальними інформаційно-пошуковими програмами, що широко використовуються всіма користувачами мережі для пошуку необхідної інформації, існує цілий ряд спеціальних програм, які можуть бути використані для проведення оперативно-розшукових заходів у мережі Інтернет відповідним правоохоронним органом.

Аналізуючи можливості програмного забезпечення, можна виділити цілий ряд спеціальних програм, які можуть бути використанні для:

- контролю за намаганнями проникнення в захищені комп’ютерні системи та мережі з можливістю протистоянню таким зломам захисту;
- негласного контролю за роботою конкретного користувача в мережі Інтернет з визначенням електронних адрес та сайтів, які відвідував користувач;
- здійснення пошуку слідів зовнішнього злому та пошуку електронної адреси і фактичного місцезнаходження комп’ютера, з якого була здійсненна атака;
- здійснення діагностики телекомунікаційних систем підключення до мережі Інтернет з метою виявлення програм небажаного доступу до інформації, можливої втрати інформації тощо;
- здійснення нелегального проникнення в захищені системи та мережі з метою отримання певної інформації щодо виявлення та попередження тяжких злочинів, що здійснюються за допомогою та в мережі Інтернет;
- проведення інших дозволених чинним законодавством оперативно-розшукових заходів за допомогою мережі.

Тобто, необхідно відмітити, що на сьогодні створено достатню кількість різноманітних програмних комплексів, які за своєю суттю є інструментами для проведення оперативно-розшукових заходів і фактично використовуються лише з цією метою.

Розглянемо, які права надані для виконання завдань оперативно-розшукової діяльності суб’єктам ОРД відповідно до чинного законодавства.

1. Опитувати осіб за їх згодою, використовувати їх добровільну допомогу. Фактична реалізація даного виду оперативно-розшукової діяльності в мережі Інтернет полягає в можливості проведення негласного опитування осіб на задану тематику за допомогою “чатів”, спілкування на різноманітних форумах, за допомогою спеціальних програм передачі текстових повідомлень (електронна пошта, SMS-повідомлення тощо). Оперативний співробітник повинен мати відповідні навички щодо спілкування через мережу. Проблемними моментами щодо достовірності отриманої інформації може стати анонімність співрозмовників. Адже, як правило, всі користувачі мають лише “нік” – “прізвисько”, яке не можна ідентифікувати, а відповідно і перевірити надану інформацію. Проте, якщо інформація отримана від декількох альтернативних джерел, то ймовірність достовірності такої інформації зростає.

2. Проводити контрольну та оперативну закупівлю і постачання товарів, предметів та речовин, у тому числі заборонених для обігу, у фізичних та юридичних осіб незалежно від форм власності з метою виявлення та документування фактів протиправних діянь. Розгалужена і така, що досить динамічно розвивається мережа Інтернет-магазинів, загальносвітова тенденція розвитку мереженої комерції говорять

про можливість здійснення оперативних закупок в Інтернет-магазинах. Проблемним питанням щодо здійснення таких закупок може стати неможливість ідентифікації продавця. Адже значна кількість товару, який зараз реалізується в мережі, має цифровий характер, і відповідно немає необхідності для безпосередньої передачі товару від продавця до покупця. Товар пересилається у вигляді відповідного файла. Але залишається можливість встановлення місця знаходження комп’ютера, з якого було здійснено відсилку такого цифрового товару.

Крім реалізації цифрових товарів, у даний час Інтернет-магазини використовуються і для реалізації “звичайних матеріальних” товарів. Для наочності можна навести приклад здійснення оперативної закупівлі підакцизних товарів через Інтернет-магазин. В Україні встановлені чіткі правила торгівлі лікеро-горілчаними виробами. Для того щоб уникнути відповідальності за збут контрафактної лікеро-горілчаної продукції, використовують мережу. Замовлення приймаються, як правило, у вечірній та нічний час та доставляються замовнику за домашньою адресою. Навіть при виявленні недоброякісної продукції, покупець не має змоги звернутись із скаргою, так як не знає, хто його обслуговував. У таких випадках є нагода застосування такого виду оперативно-розшукової діяльності, як оперативна закупка через мережу Інтернет.

3. Негласно виявляти та фіксувати сліди тяжкого або особливо тяжкого злочину, документи та інші предмети, що можуть бути доказами підготовки або вчинення такого злочину, чи одержувати розвідувальну інформацію, у тому числі шляхом проникнення оперативного працівника в приміщення, транспортні засоби, на земельні ділянки. Щодо застосування даного виду заходів до мережі Інтернет, то виникають труднощі із фіксацією та документуванням. Наприклад, на сайті з’явилась інформація, яка за своєю суттю є злочинним об’єктом (розповсюдження порнографії через Інтернет). Постає запитання: як забезпечити доказову базу розповсюдження негативного контенту, якщо розповсюджувач через деякий час повністю видаляє дану інформацію із свого сайта і її на момент фактичної перевірки немає? Виникає проблема фіксації слідів передачі інформації, розповсюдження такої інформації та її наявності на момент перевірки. Тому виникає необхідність фіксації певної сторінки сайта на окремих носіях та її підтвердження у чинному правовому колі. Одним із таких моментів документальної фіксації певної інформації на веб-сторінці може стати нотаріальне посвідчення роздрукованої сторінки із зазначенням дати та часу здійснення друку.

4. Знімати інформацію з каналів зв’язку, застосовувати інші технічні засоби отримання інформації. Міжнародний досвід здійснення державного контролю за розповсюдженням контенту в мережі Інтернет дає можливість говорити про фактично тотальний контроль за листуванням, передачею будь-яких текстових, фото-, відеофайлів через мережу Інтернет. В США всі суб’єкти надання послуг доступу до Інтернету (Інтернет-провайдери) зобов’язані забезпечити здійснення спеціальноуповноваженими органами зняття інформації за Інтернет-кореспонденцією. Спеціального дозволу на проведення таких оперативно-розшукових заходів не потрібно. Дана діяльність визначена та регламентована законодавчо.

5. Здійснювати візуальне спостереження в громадських місцях із застосуванням фото-, кіно- і відеозйомки, оптичних та радіоприладів, інших технічних засобів. Із широким розповсюдженням Інтернету та застосуванням новітніх інформаційно-комунікаційних технологій стала можливою фіксація та трансляція через встановлені в різних місцях веб-камери в режимі реального часу різноманітних подій. Досить часто особи, які потрапляють у зону зйомки такої камери, навіть не підозрюють про її існування. Тому, знаючи місця розташування таких камер, за необхідності, можна

здійснювати візуальне спостереження за певним об’єктом через мережу Інтернет та, за необхідності, все фіксувати на відповідних носіях інформації.

6. Створювати і застосовувати автоматизовані інформаційні системи. Створення спеціальних автоматизованих інформаційних систем здійснюється із різною метою. Це і накопичення, систематизація оперативної інформації з метою її подальшої ідентифікації та можливого використання. Крім того – створення спеціальних автоматизованих інформаційних систем з метою автоматичного пошуку та класифікації інформації (наприклад, за встановленими ознаками) та спеціальних систем захисту конфіденційної інформації тощо.

Сьогодні інформаційна сфера неможлива без застосування інформаційних систем та банків даних, програмного забезпечення операційних систем, прикладного та сервісного програмного забезпечення, інших інформаційних технологій, що засновані на використанні засобів обчислювальної техніки і зв’язку. Подальше удосконалення середовища накопичення інформації на різних носіях, глобальне охоплення населення засобами зв’язку, що дозволяють доставляти інформацію в будь-яку точку планети, автоматизована обробка інформації заздалегідь розробленими алгоритмами – це три технічних досягнення, на яких базуються сучасні інформаційні технології і які можуть бути використані для проведення оперативно-технічних заходів [1].

Бази даних оперативної інформації повинні слугувати для оперативних співробітників тим багажем знань, який буде сприяти проведенню оперативних заходів, із попередньою підготовкою, що повинно покращити загальний результат такої роботи.

Законом України “Про оперативно-розшукову діяльність” передбачено й інші види здійснення ОРД, проте їх не завжди можна використати в мережі Інтернет.

Аналіз чинного законодавства, що регулює оперативно-розшукову діяльність в Україні, дає можливість стверджувати про необхідність розширення кола прав правоохоронних органів щодо здійснення ОРД, зокрема в мережі Інтернет та за допомогою телекомунікаційних мереж.

В Законі України “Про оперативно-розшукову діяльність” спеціальновизначеним суб’єктам ОРД надається право здійснювати певні гласні і негласні пошукові, розвідувальні та контррозвідувальні заходи, частину яких ми вже розглянули. Проте, на сьогоднішній день залишаються нормативно не врегульованими деякі можливі оперативно-розшукові заходи, які в змозі проводити відповідні суб’єкти ОРД. Серед таких необхідно визначити перш за все негласне проникнення в захищені бази даних та захищені внутрішні мережі. Мотивуючи дану пропозицію, зазначимо, що поряд із негласним проникненням в жилі приміщення фізичних осіб, та зняттям інформації з каналів зв’язку вбачається за необхідне відокремити в нормативному акті даний оперативно-розшуковий захід з метою його правової регламентації. Додатковою аргументацію пропозиції може слугувати і той факт, що, як правило, потребу негласного проникнення в закриті бази даних необхідно ототожнювати із порушенням конфіденційності та приватності фізичних осіб. Тобто виникає необхідність правової регламентації законодавчо визначених обмежень конституційних прав та свобод людини.

Як недолік формулювання тексту чинного Закону України “Про оперативно-розшукову діяльність” хочеться відмітити розмитий, нечіткий пункт про можливість застосовувати інші технічні засоби отримання інформації.

Вся оперативно-розшукова діяльність направлена на встановлення, пошук інформації, в тому числі із застосуванням технічних засобів. Проте, на нашу думку, використання спеціальних матеріально-технічних та програмних комплексів для

проведення оперативно-розшукових заходів, пов’язаних із негласним проникненням у захищені бази даних конкретного персонального комп’ютера чи закритої мережі, не може регулюватись таким нечітким формулюванням і, відповідно, потребує внесення змін до чинного законодавства про оперативно-розшукову діяльність.

Необхідно зазначити, що негласне проникнення до житла чи до іншого володіння особи, зняття інформації з каналів зв’язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією, застосування інших технічних засобів одержання інформації проводяться лише за рішенням суду. Застосовуючи аналогію та вбачаючи необхідність захисту конституційних прав і приватності осіб при проведенні ОРД, треба визначити, що негласне проникнення до захищених баз даних чи захищених мереж має проводитися виключно за рішенням суду.

Використана література

1. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія ; ХІ.Ф. Харберюш, В.Я. Мацюк, В.А. Некрасов, О.І. Хараберюшї. – К. : КНТ, 2007. – 196 с.

2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135 / Оперативно-розшукова діяльність. Нормативно-правове регулювання / {Ю.Я. Кондратьев, О.М. Джужа, Д.Й. Никифорчук, В.В. Матвійчук] – К. : КНТ, 2005. – 552 с.

3. Овчинский А.С. Информация и оперативно-розыскная деятельность : монография / А.С. Овчинский ; под ред. заслуженного юриста Российской Федерации, доктора юридических наук, профессора В.И. Попова. – М. : ИНФРА-М, 2002. – 97 с.

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