Шраго Альона Олексіївна
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ

ПРОТИДІЯ ПОРНОГРАФІЇ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ І НФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

В Україні, як і в інших державах світу, невпинно розвиваються нові галузі економіки, що ґрунтуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема Інтернету.

Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину. Це і порнографія, шахрайства, виготовлення та поширення шкідливих програм, викрадення ідентифікаційних даних осіб та інші.

23 листопада 2001 року в Будапешті підписана Конвенція Ради Європи про кіберзлочинність (далі – Конвенція), яка була прийнята для протидії комп'ютерним злочинам та для співробітництва й координації діяльності правоохоронних органів різних держав. На сьогодні ратифікована 18 країнами та підписана 25 країнами, у т.ч. й Україною (2005) [1].

У новій редакції Стратегії національної безпеки, затвердженій Указом Президента України від 8 червня 2012 року № 389/2012, вживаються терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [2]. Слід зазначити, що в «Доктрині інформаційної безпеки України» згадувалися поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», а також питання захисту інформації від «кібернетичних атак» [3].

Механізми контролю, запобігання та розслідування злочинів у кіберпросторі дуже обмежені соціально і технологічно. 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. Отже, існує достатньо способів ускладнити припинення і розслідування злочинів.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Саме 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.

Теоретичні та практичні основи використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій, розроблені недостатньо. Аналіз спеціальної літератури та практики розслідування комп'ютерних злочинів свідчить, що існує низка проблем, пов'язаних із використанням спеціальних знань з метою пошуку, виявлення, фіксації, вилучення та дослідження слідів даної категорії злочинів у відповідності до способів їх утворення, стадії порушення кримінального провадження, при проведенні слідчих дій, розробкою спеціальних методів, засобів збирання та дослідження комп'ютерних слідів, не точно визначається предмет злочину та обставини, що підлягають доказуванню, особливо під час розслідування збуту та розповсюдження порнографії мережею Інтернет.

Проте, у практичній діяльності науково-методичні розробки не завжди схвально сприймаються. У межах проведеного нами опитування працівників кіберполіції НП України, 23 % респондентів вказали на те, що вони взагалі не звертаються до наукових рекомендацій у протидії порнографії, 43 % не використовують їх, бо вважають їх застарілими, 15 % – не ознайомлені з такими рекомендаціями, 19 % – звикли покладатися на власний досвід, з них 7 % вказали, що такі рекомендації обмежують творчий підхід до розслідування.

Однією із причин низької ефективності припинення і розслідування незаконного збуту та розповсюдження порнографії у мережі Інтернет є те, що працівники слідчих та оперативних підрозділів досі не готові до ефективного виявлення та розслідування подібних злочинів, недостатньо використовують спеціальні знання.

Серед причин високої латентності злочинів, передбачених 263н.. 301 КК України, виділяємо такі: 1) недостатня розробка понятійного апарату, що використовується в текстах відповідних статей, зокрема, відсутність чіткого визначення предмета злочинів; 2) особливий стан громадської думки, який в сучасних умовах характеризується неприйняттям названих діянь як злочинів; 3) прихований характер злочинної діяльності, відсутність очевидних її наслідків; 4) недостатня професійна підготовка працівників правоохоронних органів по виявленню і розслідуванню цих злочинів; 5) відсутність зорієнтованості правоохоронних органів на виявлення цих злочинів, які на фоні складної криміногенної ситуації (вбивства, бандитизм, розбій, зґвалтування тощо) розглядаються як другорядні і їм не приділяється належної уваги.

Закон України «Про ОРД» надає можливість використовувати права лише для виконання завдань ОРД. На законодавчому рівні не передбачено у переліку завдань профілактики злочинів, попередження та запобігання злочинам, зазначено лише припинення, про що свідчить 263н.. 1 Закону. Тобто, у Законі України «Про ОРД» наводяться два поняття, які містять суперечності, створюючи колізію правових норм: з одного боку – обов'язок оперативно-

го підрозділу здійснювати профілактику правопорушень (п. 1 ч. 1 ст. 7 Закону), з іншого – перспектива користуватися своїми правами лише для виконання завдань оперативно-розшукової діяльності (ч. 1 ст. 8 Закону), у змісті яких немає профілактики, попередження, запобігання. Відповідно, нормативно-правова регламентація профілактичної та попереджувальної діяльності оперативних підрозділів НП України має декларативний характер.

Стрімко розвивається використання Інтернету, як для вербування жертви, так і для реклами послуг. Зустрічі між жертвами та клієнтами організовуються за допомогою спеціальних веб-сайтів. Жертви швидко змінюються, залишаючись в одному місті не більше ніж на 1-2 дні. Ілюзія анонімності і масова кількість онлайн-послуг збільшує і обережність, і рентабельність цих послуг, що робить надскладною ідентифікацію злочинців із використанням лише традиційних методів поліції [4, с. 179].

Правоохоронним органам часто доводиться здійснювати первинний пошук інформації про певні об'єкти в мережі. Найбільш проблемним питанням залишається встановлення особи та визначення її місцезнаходження за тими обліковими даними, що особа лишила в мережі. Як правило, такими ідентифікаторами є адреса електронної пошти, нікнейм у форумі, профіль соціальної мережі тощо. Вказана проблема часто обумовлена підвищеним рівнем анонімності, що реалізується за допомогою різного роду розподілених ресурсів (проксі-сервери, шели) та використанням спеціалізованих захищених мереж (TOR, I2P) [5, с. 256].

Важливими правовими основами діяльності оперативних та слідчих підрозділів НП України є також норми кримінального процесуального кодексу, які, на нашу думку, сьогодні ускладнюють ефективність роботи оперативних підрозділів НП України. Так, положення 264н.. 41 КПК України забороняють співробітникам оперативних підрозділів (крім підрозділу детективів, підрозділу внутрішнього контролю НАБУ) здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокурора.

Пошукові заходи можуть здійснюватися і гласно, і негласно. Виходячи з того, що ефективність правоохоронного моніторингу соціальних мереж буде вищою за умови непоінформованості про нього суб'єктів деструктивних діянь, особливого значення набувають саме негласні заходи. Такі заходи в тому числі можуть здійснюватися оперативними підрозділами НП України.

З одного боку КПК містить прямі вказівки на необхідність проведення відповідних гласних та негласних слідчих (розшукових) дій, а з іншого – забороняє співробітникам оперативних підрозділів здійснювати процесуальні дії за власною ініціативою та звертатись з клопотанням до слідчого судді або прокурора, що, в свою чергу, знижує ефективність боротьби зі злочинами у сфері суспільної моралі, яким властива висока латентність. А тому, виникає сумнів щодо ефективності процесуалізації деяких ОРЗ у НСРД. Фактично, майже весь процес досудового розслідування сьогодні побудовано не лише

на законодавчій базі, а більшою мірою на особистих стосунках, що ставить під сумнів ефективність роботи загалом.

Із введенням в дію КПК України значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про «Конвенцію про кіберзлочинність» і Закону України «Про міліцію», то зараз така інформація віднесена до категорії документів, що містять охоронювану законом таємницю. А в розумінні статті 505 Цивільного кодексу України така 265н.формація становить комерційну таємницю, яка є одним із об'єктів інтелектуальної власності. Тому, суб'єкти протидії позбавлені можливості оперативно і своєчасно отримувати необхідну інформацію через запити правоохоронних органів. Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у тому числі і на законодавчому рівні. А тому, потребують змін положення законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів у рамках виконання зобов'язань України, узятих у зв'язку з ратифікацією «Конвенції про кіберзлочинність». Як наслідок, одним із пріоритетних напрямків є організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Сьогодні жодна держава не може ефективно протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

В умовах сьогодення постає необхідність в налагодженні на відповідній правовій основі ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

Інформаційно-аналітичне забезпечення є важливим і необхідним елементом організації оперативного пошуку ознак злочинів, пов'язаних з незаконним контентом, оскільки воно сприяє прийняттю найбільш доцільних управлінських рішень на всіх рівнях, що є однією з головних умов підвищення ефективності діяльності оперативних підрозділів НП України.

Отже, сьогодні для суб'єктів ОРД необхідною є розробка організаційно-тактичних основ проведення оперативно-розшукової діяльності у кіберпросторі та введення в дію відповідних правових механізмів їх здійснення. Окрім того, у контексті проведеного дослідження, необхідним є: 1) розробка актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі; 2) удосконалення системи інформаційно-аналітичного забезпечення (створення Єдиної інформаційно-аналітичної системи правоохоронних органів із підсистемами за напрямами, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю); 3) гармонізація кримінального законодавства про кіберзлочини на державному рівні; 4) розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що

дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонної проблеми; 5) налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні; 6) створення швидких та дієвих механізмів вирішення юрисдикційних питань у кіберпросторі; 7) удосконалення механізмів обробки електронних доказів за цією категорією кримінальних проваджень; 8) зобов'язання компаній зберігати резервні копії електронних даних для підвищення ефективності розслідування таких злочинів; 9) полегшення доступу правоохоронних органів до електронних банків даних; 10) удосконалення системи оперативного супроводження підприємств, установ та організацій, основна діяльність яких пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг; 11) забезпечення заходів безпеки на об'єктах, що призначені для передачі інформації; 12) підвищення рівня обізнаності щодо торгівлі дітьми (дитячою порнографією тощо) серед батьків та осіб, які їх замінюють, осіб, які постійно контактують з дітьми у сферах освіти, охорони здоров'я, культури, фізичної культури та спорту, судовій та правоохоронній сферах; 13) підвищення ефективності правоохоронних заходів щодо профілактики злочинів та переслідування осіб, які вчиняють цей злочин або сприяють його вчиненню; 14) створення та координування «гарячих ліній», призначених для повідомлення про факти сексуального насильства та експлуатації дітей в Інтернеті.

Розв'язання окреслених питань сприятиме підвищенню ефективності діяльності оперативних та слідчих підрозділів НП України, спрямованої на протидію загрозам інформаційного простору в цілому, та кіберзлочинам у сфері суспільної моралі зокрема, а відтак, вказані напрямки потребують подальшого поглибленого науково-методичного дослідження.

---

1. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 р. № 23-V // Відомості Верховної Ради України. – 2006. – № 39. – С. 1384. – Ст. 328.

2. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. // Офіційний вісник Президента України. – 2014. – № 16. – С. 6. – Ст. 982.

3. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 р. «Про нову редакцію Стратегії національної безпеки України» : Указ Президента України // Урядовий кур'єр. – 2012. – № 113.

4. Справочное руководство ОБСЕ по обучению полиции: Торговля людьми / серия публикаций ДТУ/ОВСВПД. Том 12. 2013. – 210 с.

5. Бандурка О.М. Оперативно-розшукова компаративістика: монографія / О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін. – Х.: Золота миля, 2013. – 352 с.