

Шраго Альона Олексіївна

ад'юнкт кафедри

Санакосв Дмитро Борисович

доцент кафедри оперативно-розшукової діяльності та спеціальної техніки

Дніпропетровського державного

університету внутрішніх справ,

кандидат юридичних наук, доцент

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

23 листопада 2001 року в Будапешті підписана Конвенція Ради Європи про кіберзлочинність (далі – Конвенція), прийнята з метою протидії комп'ютерним злочинам та співробітництва й координації діяльності правоохоронних органів різних держав [1]. На національному рівні у 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].

Боротьба з кіберзлочинністю потребує глибокого розуміння правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі і зумовлених цими характеристиками правовими і соціальними проблемами, 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 у протидії кіберзлочинам розроблені недостатньо та потребують постійного удосконалення. Аналіз спеціальної літератури та практики протидії комп'ютерним злочинам свідчить, що існує низка проблем, пов'язаних із використанням спеціальних знань з метою пошуку, виявлення, фіксації, вилучення та дослідження слідів такої категорії злочинів відповідно до способів їх утворення, стадії початку кримінального провадження, при проведенні слідчих дій, розробки 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 кіберзлочинам та порнографії зокрема, 43 % не використовують їх, бо вважають застарілими, 15 % – не знають про їх існування, 19 % – покладаються на власний досвід, з них 7 % вказали, що такі рекомендації обмежують творчий підхід до розслідування.

Проведене нами дослідження показало, що серед причин високої латентності злочинів, передбачених ст. 301 КК України, 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 й їм не приділяється належної уваги.

Матеріали практики, у т.ч. й європейської, вказують на стрімкий розвиток використання глобальної мережі для вербування жертв, організації зустрічей з ними та клієнтами, реклами послуг. Ілюзія анонімності і масова кількість онлайн-послуг збільшує обережність і рентабельність цих послуг, що робить надскладною ідентифікацію злочинців із використанням лише традиційних методів поліції [4, с. 179].

Найбільш проблемним питанням залишається встановлення особи та визначення її місцезнаходження за тими обліковими даними, що особа лишила в мережі. Такими іденти-

фікаторами є адреса електронної пошти, нікнейм у форумі, профіль соціальної мережі тощо. Означене часто обумовлене підвищеним рівнем анонімності, що реалізується за допомогою різного роду розподілених ресурсів (проксі-сервери, ШЕЛі) та використанням спеціалізованих захищених мереж (TOR, I2P). 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, зокрема, можуть здійснюватися оперативними підрозділами НП України.

Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у т.ч. 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 у налагодженні ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними органами та правоохоронними органами інших країн, з метою документування злочинних груп із міжнародними зв'язками.

Важливим і необхідним елементом організації оперативного пошуку ознак злочинів, пов'язаних з незаконним контентом, є також інформаційно-аналітичне забезпечення, оскільки воно сприяє прийняттю найбільш доцільних управлінських рішень на усіх 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 здійснення оперативно-розшукової діяльності у кіберпросторі та введення у дію відповідних правових механізмів для цього. Окрім того, необхідним вважаємо: 1) розробку 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 напрямками, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю); 3) гармонізацію кримінального законодавства про кіберзлочини на державному рівні; 4) імплементацію міжнародних процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і подавати електронні докази з урахуванням транскордонної проблеми; 5) налагодження співробітництва 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 мережі Інтернет.

Розв'язання окреслених питань сприятиме підвищенню ефективності діяльності оперативних та слідчих підрозділів НП України, спрямованої на протидію загрозам інформаційному простору в цілому та кіберзлочинам у сфері суспільної моралі зокрема, а тому 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. 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. 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. Оперативно-розшукова компаративістика: монографія / О.М. Бандурка, М. М. Перепелиця, О. В. Манжай та ін. Харків: Золота миля, 2013. 352 с.

Гулян Амест Давидівна
студентка юридичного факультету

Науковий керівник –
Скок Олександра Сергіївна
доцент кафедри
кримінально-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

КРИМІНАЛЬНО-ПРАВОВІ ЗАСАДИ ЕКСТРАДИЦІЇ

Здійснювана в Україні судово-правова реформа зумовлює необхідність наповнення новим змістом традиційних положень кримінального права і появу нових інститутів, які мають безпосередньо практичне значення.

Одним з таких інститутів є інститут екстрадиції, сутність якого полягає у передачі особи державою, на території якої вона перебувала, іншій державі для притягнення її до кримінальної відповідальності або для виконання вироку суду [1, с. 176]. Проте в національному законодавстві інститут екстрадиції чітко не визначений, що створює значні труднощі у боротьбі зі злочинністю, особливо організованою та транснаціональною. Недосконалість механізму видачі особи в українському кримінальному законодавстві не сприяє забезпеченню одного із завдань кримінального судочинства, яке передбачає притягнення до відповідальності кожного, хто вчинив злочин. Проблематика екстрадиції залишається актуальною поряд з іншими питаннями, які виникають у сфері боротьби зі злочинністю.

Відповідно до завдань кримінального судочинства особа, яка вчинила злочин, має бути притягнута до кримінальної відповідальності. Згідно з ч. 1 ст. 6 КК України особа, яка вчинила злочин на території України, підлягає кримінальній відповідальності за КК України [2]. Злочин визнається вчиненим на території України, якщо його було почато, продовжено, закінчено або припинено на території України, якщо його виконавець або хоча б один із співучасників діяв на території України (ч. 2, 3 ст. 6 КК України). Проте особа після вчинення злочину може перебувати за межами України, і для вирішення питання про її кримінальну відповідальність та покарання вона має повернутися в Україну. Це можливо і добровільно, зокрема коли така особа не вважає себе винною у вчиненні злочину і сподівається довести це особисто за допомогою свого захисника, ставши активним учасником кримінального провадження. Але найчастіше особи, які вчинили злочини в Україні, опиняються за її межами з метою ухилитися від кримінальної відповідальності і покарання за вчинені ними злочини [3, с. 217]. Саме за таких умов й постає питання щодо необхідності застосування процедури екстрадиції.

Взагалі, екстрадиція здійснюється відповідно до норм міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, а також положень національного законодавства. Так, до міжнародних актів, зокрема, можна віднести: Загальну декларацію прав людини 1948 р., Статут ООН 1945 р., Європейську конвенцію про захист прав людини та основоположних свобод 1950 р., Конвенцію про попередження злочину геноциду та покарання за нього 1948 р., Конвенцію проти транснаціональної організованої злочинності 2000 р., Європейську конвенцію про видачу правопорушників 1957 р., Конвенцію про правову допомогу у цивільних, сімейних та кримінальних справах (Мінську конвенцію) 1993 р., Додатковий протокол до Конвенції 1993 р., низку двосторонніх договорів України щодо видачі, згода на обов'язковість яких надана Верховною Радою України [4, с. 133].

Слід додати, що Конституція України окремим положенням цього правового інституту надала характеру конституційної норми. Так, відповідно до ч. 2 ст. 25 Конституції