СЕКЦІЯ 6
ВИЯВЛЕННЯ, ПОПЕРЕДЖЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ТОРГІВЛІ ЛЮДЬМИ, ВЧИНЕНИХ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 343.541

Сергій Васильович ДЕМЕДЮК,
кандидат юридичних наук,
начальник Департаменту кіберполіції Національної поліції України;
Тетяна Сергіївна ДЕМЕДЮК,
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ

ВИЯВЛЕННЯ ОСІБ, ЩО ЗАЙМАЮТЬСЯ РОЗПОВСЮДЖЕННЯМ ДИТЯЧОЇ ПОРНОГРАФІЇ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Україна є одним з лідерів у світі за розповсюдженням дитячої порнографії у мережі Інтернет. Щороку в нашій державі до кримінальної відповідальності за розповсюдження дитячої порнографії притягуються сотні осіб. Стрімкий розвиток інформаційних технологій та комп'ютерної техніки спричинив утворення принципово нових схем вчинення злочинів, пов'язаних із розповсюдженням продукції порнографічного характеру через всесвітню мережу Інтернет, що передбачено статтею 301 Кримінального кодексу України. Особливо суспільно небезпечними проявами таких відносин є втягнення до злочинних діянь у цій сфері неповнолітніх та малолітніх, які стають не тільки знаряддям злочину, а й об'єктом наруги, примушування до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру з розбещенням, зґвалтуванням, застосуванням до них різного роду насильства та сексуальної експлуатації.

Категорія злочинів, пов'язаних із дитячою порнографією, є досить специфічною, тому вимагає принципово нового підходу оперативних працівників та слідчих до їх попередження та розслідування. По-перше, великого значення для доказування обставин набуває технічна інформація, що нетипово для інших видів злочинів. Це вимагає від працівників певного рівня знань у сфері комп'ютерної техніки, засобів комунікації тощо. По-друге, ефективне здійснення оперативно-розшукової та процесуальної діяльності у справах цієї категорії передбачає проведення комплексу заходів, які ще недостатньо поширені в службовій діяльності органів розслідування (оперативна закупівля через мережу Інтернет). По-третє, у багатьох випадках

діяльність злочинців виходить за межі України, тому виникає необхідність міжнародного співробітництва.

Департамент кіберполіції співпрацює з Міжнародною оперативною групою по боротьбі з дитячою порнографією ФБР США, можливості якої використовуються при документуванні протиправної діяльності транснаціональних злочинних груп. В Інтерполі створено автоматизовану базу даних зображень дітей, які стали жертвами сексуальної експлуатації в Інтернеті. Інформаційні масиви накопичують відомості про ідентифікованих та неідентифікованих потерпілих від сексуального насильства і доступні для всіх країн – учасниць Інтерполу.

Ефективна робота оперативних і слідчих підрозділів у протидії злочинам, пов'язаним із виготовленням та розповсюдженням дитячої порнографії у всесвітній комп'ютерній мережі Інтернет, вимагає встановлення осіб, причетних до діяльності того чи іншого інтернет-ресурсу, та спостереження за діями цих осіб з одночасним їх документуванням. У ході цієї роботи необхідно встановити:

– кому належить той чи інший сайт або електронна поштова скринька;

– реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостінгу, як користувача сайту;

– адресу, телефонні номери та інші реквізити власника сайту;

– IP-адресу, яку використовували для створення та поповнення змісту сайту;

– інформацію щодо змісту сайту та користування ним тощо.

Кожен комп'ютер у мережі має свою унікальну адресу, яка називається IP-адреса (адреса інтернет-протоколу). Під час реєстрації мережі в Інтернет їй виділяється мережний ідентифікатор залежно від класу. Ідентифікація ж вузлів у підмережах мережі здійснюється організацією-власником.

Коли особа підключається до інтернет-мережі, її комп'ютер стає частиною мережі, і йому надається унікальна IP-адреса. Отримання IP-адреси здійснюється під час кожного підключення, але ця адреса кожного разу має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення.

Статичні IP-адреси, як правило, закріплені за тими вузлами мережі Інтернет, що повинні бути присутніми у мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів Інтернету.

Хоча комп'ютерна система IP-адресації здається цілком прийнятною в усіх відносинах, для людини форма подачі цієї інформації вважається не зовсім зручною. Коли комп'ютеру дається команда відкрити сторінку, то вводиться URL (адреса інтернет-ресурсу), це змушує комп'ютер звертатися за довідкою до іншого комп'ютера щоб визначити, яка IP-адреса відповідає введеному доменному імені. Цей «довідковий» комп'ютер називається сервером

DNS (Domain Name System), який є службою каталогізації доменних імен. Таблиця відповідності доменних імен IP-адресам розміщається на багатьох DNS-серверах, що послідовно опитуються в процесі пошуку того чи іншого значення.

Інформацію про особу, яка зареєструвала та використовує доменні імена, може надати компанія-реєстратор. У більшості випадків отримання домену здійснюється автоматизовано і на умовах публічного договору, тому письмовий договір із клієнтом не укладається. Однак, процедура реєстрації передбачає отримання деяких відомостей про власника домену.

Щоб довідатися про IP-адресу сайту, доменне ім'я якого відомо (і взагалі довідатися, чи існує така адреса), можна скористатися програмою Ping (Packet Internet or Inter-Network Groper), що входить у комплект Windows.

Отримання інформації про адресу електронної пошти суттєво відрізняється від перевірки відомостей про сайти. Дані щодо інтернет-сайту отримати легше тому, що для постійного доступу він має статичну адресу та розташований на технічних ресурсах провайдера, які надаються клієнтам за плату. Ця послуга має назву «хостінг» (англ. «hosting» – хазяйнувати) – надання провайдером власних технічних ресурсів для розміщення та роботи сайтів.

З метою перевірки адреси електронної пошти, якими користуються зловмисники, доцільно провести моніторинг із використанням пошукових систем і загальнодоступних сервісів. Подальші заходи залежать від поштової служби, якою користується фігурант, оскільки наші можливості обмежені співпрацею з українськими компаніями, наприклад, Ukr.net, Gala.net, TeNet та іншими. Без отримання дозволу суду на проведення заходів, які обмежують права та свободи громадян, можливо отримати таку інформацію:

1. Адреса, телефонні номери та інші реквізити абонента.
2. IP-адреси, які використовувалися для створення цього облікового запису.
3. IP-адреси, які використовуються для з'єднання з цим обліковим записом.
4. Реєстраційні дані (logs) та абонентська інформація про користувача облікового запису (електронної поштової адреси).
5. Відомості про обліковий запис (електронну поштову адресу), на який пересилається повідомлення після його отримання (робиться операція «Forward»).

У випадку використання правопорушником електронної поштової адреси є велика ймовірність, що на перші два запитання відповіді в провайдера не буде або інформація буде неправдивою. Це обумовлено тим, що більшість електронних поштових адрес надаються безкоштовно і користувач майже ніколи не заповнює реквізити. Останні три запитання дають інформацію про осіб, які можуть надати

додаткову інформацію стосовно користувача електронної поштової адреси, якого необхідно встановити, інші електронні поштові адреси, які він може використовувати, та його особисті адреси.

Тут будуть отримані динамічні IP-адреси інших провайдерів, з яких здійснював свою діяльність користувач електронної поштової адреси, тому дуже важливо знати точний час стосовно кожної використаної адреси. Згідно з цією інформацією необхідно за допомогою сервісу Whois установити провайдера, який надавав послугу з використання мережі Інтернет для користувача електронної поштової адреси, та направити до нього запит або отримати таку інформацію за допомогою ухвали слідчого судді. Відповідь на це запитання надасть можливість установити фактичну адресу користувача електронної поштової адреси.

Але якщо електронна поштова адреса створена навмисно для протиправних дій, правопорушник може користуватися нею з інтернет-клубів (кафе, орендованих квартир, готелів тощо), тому необхідно буде встановити:

1. Комп'ютер у внутрішній локальній мережі клубу (кафе або інше місце), з якого правопорушник здійснював свою діяльність.

2. Який адміністратор закладу був на зміні під час виходу правопорушника в мережу Інтернет.

3. Осіб з числа інших клієнтів, які в той час знаходились поблизу комп'ютера правопорушника.

4. Інший обслуговуючий персонал клубу (кафе, готелю тощо), який міг запам'ятати правопорушника (охоронець, бармен, прибиральниця тощо).

Зазначених осіб необхідно опитати та встановити особу правопорушника.

Зміст електронного листування особи, перелік її контактів або паролі доступу до скриньки можливо отримати виключно за ухвалою слідчого судді і в установленому законом порядку.

Найбільш ефективним способом, який дозоляє отримати первинні дані про вчинення таких злочинів, є систематичний і цілеспрямований моніторинг загальнодоступних інформаційних ресурсів.

У багатьох випадках перед органами розслідування постає завдання доказати факт використання конкретного комп’ютера для доступу до інтернет-ресурсів. Така потреба, зокрема, виникає, коли для з’єднання із глобальною мережею використовувалася динамічна IP-адреса, яка могла бути надана необмеженому колу осіб (наприклад, у разі використання безпровідного з’єднання Wi-Fi або підключення до мережі через засоби стільникового зв’язку тощо). У таких випадках слід відслідкувати MAC-адресу комп’ютера зловмисника. MAC-адреса, або фізична адреса комп’ютера, – це незмінний ідентифікаційний номер пристрою, за допомогою якого здійснюється з’єднання з мережею. Він є індивідуальним для кожного комп’ютера і практично не піддається зміні.

Слід відзначити, що під час вчинення злочинів зазначеної категорії для зашифровки схеми руху коштів зловмисниками використовуються віртуальні трансферні системи, такі як Webmoney, E-passport, Yandex-деньги та інші. Для цього злочинці відкривають власні інтернет-гаманці шляхом створення облікових записів у адміністраторів систем. Номер інтернет-гаманця, як правило, не приховується. Він може міститися в рекламному оголошенні, на сайті інтернет-крамниці або повідомлятися в ході спілкування з покупцями.

Номер гаманця дозволяє отримати деяку інформацію про його власника і відомості, які в подальшому можна використати в суді як докази діяльності підозрюваного.

Оператор трансферної системи, як правило, має відомості про програмне забезпечення, яким клієнт користується для здійснення операцій по гаманцях. Такі клієнтські програми є специфічними та можуть завантажуватися на комп'ютер користувача з сайтів оператора. Відповідна інформація також може бути надана оператором за запитом і матиме доказове значення після вилучення комп'ютерної техніки, яка використовувалася для вчинення злочину, та проведення комп'ютерно-технічної експертизи.

Отримана інформація у подальшому дозволить з'ясувати додаткові відомості про фігуранта: встановити його особу та місце проживання, номер мобільного телефону, комп'ютер, який використовується для з'єднання з мережею Інтернет. У деяких випадках для підтвердження сертифікатів представники трансферних систем вимагають від клієнтів надання копій документів, які підтверджують особу (найчастіше – паспорту), отже є вірогідність отримання за запитом повних паспортних даних власника інтернет-гаманця.

Як уже зазначалося, відомості про осіб, які представляють оперативний інтерес, можливо отримати шляхом елементарного використання пошукових систем. У поле пошуку рекомендується вводити будь-які ідентифікуючі дані об'єкта: номери телефонів, гаманців, облікових записів інтернет-пейджерів, електронні та поштові адреси, прізвища або вигадані для спілкування в мережі імена, назви суб'єктів підприємницької діяльності тощо.

Серед інтернет-ресурсів, на яких може міститися інформація, що становить оперативний інтерес, слід визначити такі:

– сайти, які відкрито пропонують послуги сексуального характеру за гроші або роблять це завуальовано: під виглядом масажних салонів, VIP-відпочинку, ескорт-послуг тощо;

– веб-сторінки з дошками оголошень незалежно від спеціалізації («куплю», «продам», «пропоную роботу» і т. д.) або регіональної спрямованості;

– форуми різноманітної тематики;

– соціальні мережі;

– сайти знайомств, на яких розміщуються анкети користувачів.

Щоб закріпити процесуальне значення інформації, здобутої під час проведення розшукових заходів, необхідно належним чином оформити документи про отримання та фіксацію інформації. За наявності відкритого доступу до змісту сайту слід оформити протокол огляду в присутності понятих із застосуванням відеозапису або програм, які фіксують зображення, що виводиться на екран. У разі використання програм «SnagIt», «Camtasia» отримані відомості необхідно записати на оптичний носій без можливості перезапису (CD-R) та долучити диск до протоколу як додаток.

Отже, для припинення та розкриття кримінального правопорушення щодо розповсюдження дитячої порнографії, вчиненого із застосуванням інформаційних технологій, потрібно ідентифікувати комп'ютер, в якому зберігається і з якого розповсюджується продукт дитячої порнографії. В подальшому слід установити осіб, які зберігають, адмініструють та розповсюджують ресурси, на яких розміщується контент із дитячою порнографією.

Список бібліографічних посилань

1. Кримінальний кодекс України : закон України від 5 квіт. 2001 р. № 2341-III, зі змін. станом на 14.03.2018 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/ show/2341-14 (дата звернення: 31.10.2018).

2. Кібербезпека дітей в Інтернеті : Про що мають дбати батьки, школа // Womo. URL: http://womo.ua/kiberbezpeka-ditey-batki-shkola-derzhava/ (дата звернення: 31.10.2018).

3. Конвенція Ради Європи про кіберзлочинність : ратиф. із застереженнями і заявами законом України від 7 верес. 2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5–6. Ст. 71.

4. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії : закон України від 03.04.2003 № 716-IV // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/995_b09 (дата звернення: 31.10.2018).

5. Виявлення, документування та притягнення до відповідальності членів організованих злочинних груп та окремих осіб, що займаються виготовленням, збутом та розповсюдженням продукції порнографічного характеру : навч.-метод. рек. / Управління боротьби з кіберзлочинністю МВС України. Київ, 2013. 36 с.

Одержано 02.11.2018