Хижняк Євген Сергійович

Національний університет «Одеська юридична академія»,

доцент кафедри криміналістики,

кандидат юридичних наук

ПРОЦЕС ВСТАНОВЛЕННЯ ОСОБИСТОСТІ ЗЛОЧИНЦІВ, ЯКІ ВЧИНЯЮТЬ ЗЛОЧИНИ В МЕРЕЖІ ІНТЕРНЕТ

Існування людини у віртуальному просторі виражається у використані нею спеціальних програм, технічних засобів, комп'ютерних та телефонних додатків, які спрощують та оптимізують життя людини. Такими засобами є електронна пошта, електронні платіжні системи, кредитні та платіжні картки, записи в електронних книгах, календарі, соціальні та пошукові мережі тощо, внаслідок експлуатації яких незалежно від волі людини в електронній мережі залишаються віртуальні сліди, що генеруються використовуваними людиною електронними пристроями. Стаючи частиною суспільного життя, віртуальний простір стає частиною злочинного світу, де накопичені криміналістикою знання стають недостатніми для виконання завдань кримінального провадження.

У зв'язку із цим, проблемою сучасної криміналістики стають питання пошуку віртуальних слідів, способів їх вилучення та можливостей їх використання в процесі розслідування кримінальних правопорушень, зокрема, встановлення особистості злочинця, який вчиняє злочин в мережі Інтернет.

Встановлення особистості злочинця, який вчиняє неправомірну діяльність в мережі Інтернет, розпочинається із фіксування самого факту неправомірної дії. На думку Двойнікова О.О., у разі виявлення факту розміщення забороненої інформації в глобальній мережі правоохоронними органами, під час фіксування готуються такі документи, що підтверджують факт знаходження протиправного контенту на сайті: 1) рапорт (лист) працівника органів внутрішніх справ про виявлення та встановлення наявності знаходження протиправної інформації на

сайті; 2) протокол зі скріншотами (копії сторінки сайту з екрана), що підтверджує наявність протиправної інформації на сайті; 3) документ (файл) для перегляду сторінки сайту в режимі онлайн; 4) додається посилання на сторінку сайту у каталозі обраного в Microsoft Internet Explorer; 5) створюється копія сторінки сайту на жорсткому диску за допомогою спеціальної утиліти; 6) готується інформаційна довідка про ідентифікаційні дані сайту (IP-адреса, URL), інтернет-провайдера (електронна адреса, номери телефонів) тощо [1, С. 220].

На підставі встановленого факту розміщення інформації в мережі Інтернет, що також може бути здійснено як за ініціативою слідчого, так і на підставі заяви зацікавлених осіб, слідчий відкриває кримінальне провадження. Першочерговою слідчою дією, яку повинен здійснити слідчий є слідчий огляд веб-сайту в порядку, передбаченому ст. 237 КПК України, на предмет наявності чи відсутності факту вчинення кримінального правопорушення.

Під час огляду веб-сайту, у разі відсутності в слідчого спеціальних знань, слідчий повинен залучати до огляду відповідного спеціаліста. У протоколі огляду слід зазначати серійний номер службового комп'ютера, назву та версію операційної системи, яка встановлена на даному комп'ютері, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі Інтернет [2, С. 187].

Після встановлення IP-адреси домену, найменування інтернет-провайдера, який надає доступ до веб-сайту, та його місцезнаходження керуючись нормами глави 15 КПК України, слідчий повинен отримати тимчасовий доступ до документів, що знаходяться у провайдера телекомунікацій та містять охоронювану законом таємницю, а саме: інформацію про особу, яка зареєструвала веб-сайт, IP-адресу електронно-обчислювальної машини, з якої було здійснено реєстрацію веб-сайту, IP-адресу електронно-обчислювальної

машини, з якої здійснювалось управління веб-сайтом та наповнення веб-сайту забороненим контентом [1, С. 221].

Після встановлення інформації про особу, яка зареєструвала веб-сайт та IP-адреси електронно-обчислювальної машини, з якою здійснюється адміністрування сайту, слідчий повинен отримати доступ до персональних даних такої особи. Особа, яка зареєструвала сайт, та особа, яка здійснює його адміністрування та наповнення, можуть не співпадати, а тому інтернет-провайдер може надати лише IP-адресу електронно-обчислювальної машини без зазначення будь-яких персональних даних.

У зв'язку із цим, слідчий на підставі відомої IP-адреси ЕОМ, з якої здійснюється доступ до певного веб-сайту, за допомогою ресурсів «2ip» та «whois» встановлює інтернет-провайдера, який надає доступ до Інтернету особі із вищезазначеною IP-адресою ЕОМ. Після цього, слідчий отримує в слідчого судді тимчасовий доступ до інформації та документів іншого інтернет-провайдера стосовно персональних даних особи за конкретною IP-адресою.

При кожному візиті абонентом мережі Інтернет журнал сервера, який знаходиться у фізичному володінні Інтернет-провайдера, зберігає наступну інформацію: клієнтські IP-адреса/місце розташування, дату і час запиту, конкретні адреси запитаних сторінок, код HTTP, кількість байт, переданих користувачеві, агент браузера у користувача.

Отже, на даному етапі слідчому стає відома IP-адреса домену сайту, на якому розповсюджено заборонену інформацію, та інтернет-провайдер, який забезпечує доступ до такого сайту, IP-адреса ЕОМ, з якої було розповсюджено таку інформацію, інтернет-провайдер такої особи, фізична особа, якій належать IP-адреса, її місце розташування, дата і час розповсюдження заборонених матеріалів, інші дії, які вчинялись на веб-сайті з конкретної IP-адреси ЕОМ.

Для забезпечення точної ідентифікації особи злочинця, слідчий повинен отримати фізичний доступ до електронно-обчислювальної машини, з якої

здійснювалось розповсюдження інформації. На підставі інформації про ймовірного злочинця та його місця розташування слідчий звертається до слідчого судді із клопотанням щодо отримання ухвали про обшук за вказаною адресою та проведення інших слідчих (розшукових) дій.

В пам'яті ЕОМ зберігається інформація про вчинене кримінальне правопорушення, зокрема матеріали, які були незаконно розповсюджені, інформація про відвідувані веб-сторінки, на яких було розповсюджено заборонену інформацію тощо. Тому слідчий на підставі даних, отриманих від інтернет-провайдера, та даних ЕОМ остаточно ідентифікує особу злочинця, встановлює обставини, які мають значення для кримінального провадження та збирає необхідні докази.

Таким чином, слідчий на підставі інформації про веб-сайт, на якому розміщені заборонені матеріали, викладені викрадені об'єкти авторського та суміжних прав тощо, може встановити особистість злочинця, який вчинив кримінально карні діяння.

Іншим способом встановлення особи може виступати пошук інформації за її мережевими ідентифікаторами, які особа залишила в мережі. Як правило, такими ідентифікаторами виступають адреса електронної поштової скриньки, нікнейм у форумі, профіль соціальної мережі тощо. Перш за все, необхідно скористатися можливостями інтегрованої інформаційно-пошукової системи органів внутрішніх справ. У рамках використання даного способу також можуть бути застосовані різні пошукові системи, такі як Google, Rambler, Yahoo тощо.

Пошук доцільно продовжити в соціальних мережах, таких як «Фейсбук», «Instagram», «Twitter» тощо. Користувачі активно розміщують на своїх сторінках інформацію особистого характеру: номери телефонів, адреси, місце роботи, посаду, місце свого знаходження, фотографії. На підставі інформації з соціальних мереж можливо встановити стать, вік, майновий стан особи, освіту, сферу інтересів, фізичне місцезнаходження особи в той чи інший час.

Додатковим способом пошуку особи є використання сервісів «FaceSearch» та інформаційного ресурсу «Radaris», які забезпечують пошук зображень облич. Крім того, в якості додаткових джерел криміналістичної інформації можливо використовувати інформаційні ресурси «nomer.org», «lookup.com», приватні бази суб'єктів маркетингових досліджень.

Незважаючи на існуючі способи ідентифікації особистості злочинця, які вчиняють злочини в мережі Інтернет, на сьогоднішній час окремими злочинцями використовуються спеціальні засоби анонімізації даних в глобальній мережі, такі як VPN-технології, відкриті проксі-сервери, мережа TOR, які шифрують дані, приховують віртуальні сліди, що унеможливлює або значно ускладнює розслідування злочинів, вчинених за допомогою таких технологій.

Отже, основним способом ідентифікації злочинця є встановлення його особистості за допомогою IP-адреси домену сайту, на якому розміщено заборонено інформацію, та IP-адреси електронно-обчислювальної машини, за допомогою якої здійснювався вихід в глобальну мережу. Отримання такої інформації здійснюється за допомогою відкритих інтернет-ресурсів та слідчих дій, спрямованих на отримання доступу до речей та документів відповідних інтернет-провайдерів. В процесі встановлення особистості злочинця слідчий повинен використовувати облікові дані, які особа залишила за собою в мережі. Пошукові системи, відкриті бази даних, соціальні мережі стають одним з головних джерел криміналістичної інформації, на підставі якої встановлюється особистість злочинця, його психофізіологічні риси, соціальний статус, місцезнаходження тощо.

Список використаної літератури:

1. Двойніков О.О. Кримінально-процесуальні особливості встановлення особи, яка вчинила злочин за допомогою Інтернет-сайту / О.О. Двойніков //

Актуальні питання розслідування кіберзлочинів. Матеріали міжнародної науково-практичної конференції. – Х., 2013 р. – С. 218 – 222.

2. Коваленко А.М. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров’я журналіста / А.М. Коваленко // Вісник Національної академії правових наук України. – № 1 (88). – 2017 – С. 182-191.