УДК 343.9

Євген Хижняк,
канд. юрид. наук, доцент кафедри криміналістики
Національного університету «Одеська юридична академія»

ІДЕНТИФІКАЦІЯ ОСОБИСТОСТІ ЗЛОЧИНЦЯ ЗА ВІРТУАЛЬНИМИ СЛІДАМИ В МЕРЕЖІ ІНТЕРНЕТ

У статті досліджено способи встановлення особистості злочинців, які вчиняють кримінальні правопорушення в мережі Інтернет, можливості використання мережевих ідентифікаторів та інших віртуальних слідів в процесі встановлення суб'єктів злочину. Проаналізована роль та значення інформаційних технологій та соціальних мереж в процесі розслідування кримінальних правопорушень. Досліджені найбільш оптимальні та раціональні прийоми, які складають комплекс дій слідчого та оперативних підрозділів, спрямованих на встановлення осіб, що вчинили злочини в мережі Інтернет. Визначені основні проблеми та складнощі, які перешкоджають ефективному встановленню суб'єктів злочину в глобальній мережі.

Ключові слова: суб'єкт злочину, встановлення злочинця, Інтернет, інформаційні технології, ідентифікація злочинця.

Постановка проблеми. Закономірним наслідком розвитку інформаційних технологій стає їх глобальне впровадження в усі аспекти життєдіяльності людини. Людина в більшій чи меншій мірі існує одночасно в двох просторах – реальному і віртуальному. Якщо перший був предметом вивчення криміналістики протягом усього часу її існування, то другий все ще знаходиться на стадії усвідомлення необхідності його дослідження та поступового освоєння.

Стаючи частиною суспільного життя, віртуальний простір стає частиною злочинного світу, де накопичені криміналістикою знання стають недостатніми для виконання завдань кримінального провадження.

У зв'язку з чим, актуальним завданням сучасної криміналістики стають питання ідентифікації особистості злочинця по віртуальним слідам, які він залишив в мережі Інтернет, можливості використання глобальної мережі для дослідження особистості злочинця, виконання діагностичних завдань, які стоять як перед кожним криміналістом окремо в процесі розслідування злочинів, так і перед криміналістикою як наукою в цілому.

Стан дослідження. Досліджуваній у даній статті проблематиці, а також її окремим питанням присвячували свої праці такі науковці, як: В.В. Білоус, В.Б. Вєхов, А.Ф. Волобуєв, О.О. Двойніков, О.В. Захарченко, Н.С. Козак, О.Є. Користін, О.В.Манжай, І.А. Осятинська, В.М. Струков, В.В. Торяник, Н.Н. Федотов, В.Ю. Шепітько, О.М. Юрченкота ін.

Метою даної **статті** є дослідження способів встановлення особистості злочинців, які вчиняють кримінальні правопорушення в мережі Інтернет, характеристика комплексу дій слідчого та оперативних підрозділів, спрямованих на встановлення таких осіб, а також дослідження ролі та значення інформаційних технологій та соціальних мереж в процесі розкриття злочинів.

Для досягнення поставленої мети визначено наступні завдання:

- дослідити основні способи ідентифікації злочинців, які вчиняють кримінальні правопорушення в мережі Інтернет;
- визначити роль інформаційних технологій та можливості їх використання в процесі розкриття кримінальних правопорушень;
- дослідити можливості використання соціальних мереж в процесі збирання криміналістичної важливої інформації;
- охарактеризувати алгоритм дій слідчого та оперативних підрозділів, які спрямовані на встановлення особистості злочинців;
- дослідити основні проблеми та складнощі встановлення особистості злочинців в мережі Інтернет.

Виклад основних положень. 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.

Виступаючи творцем і розповсюджувачем власного контенту та споживачем чужого, людина неминуче залишає в кіберпросторі віртуальні сліди своєї діяльності. За цими слідами можна встановити не тільки фізичні параметри часу та місця вчинення тієї чи іншої дії, а й з високим ступенем імовірності вирішити низку діагностичних завдань з формування психологічного профілю відображеного суб'єктата прогнозування його майбутньої поведінки [8, с. 6].

Особливість віртуального простору полягає в тому, що взаємодіючі в ньому об'єкти, які беруть участь в процесі утворення слідів, не мають зовнішньої будови. Накопичені знання

криміналістичної трасології стають практично непридатними для дослідження віртуальних слідів. Віртуальні сліди – це будь-які зміни комп'ютерної інформації, пов'язані з подією злочину, зафіксовані на матеріальних носіях комп'ютерної техніки. Вони не мають матеріальної форми існування, існують лише на технічних носіях та мають складну інформаційну структуру, в якій поряд зі значимою кримінально-релевантною інформацією міститься значний обсяг допоміжних даних, що відповідають за цілісність і доступність комп'ютерної інформації віртуального сліду.

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 [2, 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 [3, с. 187].

Під час огляду веб-сторінки слідчий повинен зібрати максимально можливий об'єм інформації, який надасть змогу ідентифікувати особу злочинця. Обов'язково в ході огляду слідчий повинен встановити домен сайту, вказати URL веб-сторінки, який завжди є індивідуальним, зазначити стандартні реквізити електронного документа: назву, автора, псевдонім, час створення електронних документів, якщо такі відомі, призначення документа, стислий зміст та викладені в ньому обставини, які мають значення для розслідування злочину.

Інформація, що є доступною у мережі Інтернет, у тому числі й та, що міститься на вебсайтах, фізично розміщена на комп'ютерному обладнанні, об'єднаному каналами зв'язку з цією мережею, і кожне таке обладнання має IP-адресу – ідентифікатор (унікальний номер, який складаєтьсяз набору чотирьох 8-бітних чисел), що використовується для адресації комп'ютерів у електронні мережі.

Домен сайту завжди є відкритим та відомим для будь-якого абонента мережі. На підставі найменування домену сайту слідчий може встановити IP-адресу домену та інтернет-провайдера, його найменування та місцезнаходження серверу, на якому зберігаються дані сайту. Встановлення вищезазначених даних здійснюється за допомогою інтернет-ресурсів «2ip» та «whois», які знаходяться у відкритому доступі, а тому будь-яка людина може самостійно встановити інтернет-провайдера та місцезнаходження будь-якого сайту.

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 вебсайту забороненим контентом [2, 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 вищезазначених 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 фі-

зичному 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.

Провайдер може також записати IP-адреси / розташування відвіданих сайтів, скільки даних передано і що конкретно було передано і отримано. Поки дані не зашифровані, інтернет-провайдер зможе бачити, які конкретно дії здійснювалися, яка інформація отримувалась та передавалась. Наприклад, відеохостинг «Youtube» не шифрує трафік, а тому інтернет-провайдер може спостерігати, що саме переглядає абонент. В свою чергу, соціальна мережа «Facebook» свій трафік шифрує, а тому в третіх осіб, окрім абонентів та службових осіб організації «Facebook», доступ до такої інформації закритий.

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.

В цьому напрямку цікавими є дослідження вчених французького державного інституту досліджень в інформатиці та автоматиці INRIA, в якому вони дійшли висновку, що історія веб-браузера кожного користувача унікальна. Вони зазначають, що історія запитів в браузері – це віртуальні сліди, аналогічні відбиткам пальців людини. За кількома постійними запитами можна визначити, хто саме їх зробив.

На підставі дослідження історії запитів близько 370000 інтернет-користувачів, французькі вчені проаналізували різні комбінації запитів і частоту відвідування певних сайтів кожного з учасників дослідження. Результати показали, що для більшості користувачів – 68%, історія відвідувань веб-браузера унікальна. Дослідження показали, що на підставі перегляду чотирьох сайтів у 97% випадків можна ідентифікувати конкретну людину [9].

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.

Одним із способів встановлення особи за мережним ідентифікатором є використання систем відновлення паролів різних ресурсів. Зокрема, таким чином можна встановити номери телефонів, віднайти профіль особи у соціальних мережах тощо. У подальшому, аналізуючи зміст та геопозначки відповідних фотографій можна встановити місця перебування особи у певний проміжок часу. Знаючи місця пересування особи, можна у 95 % випадків однозначно її ототожнити, що на практиці було доведено дослідниками з Масачусетського технологічного інституту і Католицького університету в Левені [4, с. 257].

Процес встановлення особистості злочинців, які вчиняють злочини в мережі Інтернет, стикається із рядом певних проблем, які перешкоджають встановленню суб'єкта того чи іншого злочину. Сутність таких проблем полягає у застосуванні злочинцями таких технічних засобів, програмних комплексів тощо, які або забезпечують повну анонімність злочинця в мережі Інтернет або значно ускладнюють процес ідентифікації таких осіб.

1. Застосування VPN-технологій. VPN (від англ. Virtual Private Network) – це технологія, сутність якої полягає у створенні безпечного та зашифрованого з'єднання над менш

безпечним з'єднанням, таким як Інтернет. Технологія VPN була розроблена як спосіб дозволити віддаленим працівникам та філіям безпечно отримувати доступ до корпоративних даних, внутрішніх програм та інших ресурсів.

VPN створює захищене тунельне з'єднання з використанням спеціальних VPN-протоколів – маскує справжню IP-адресу користувача за своїм власним – шифрує всі дані користувача і передає їх захищеним тунелем, що дозволяє використовувати Інтернет анонімно. У зв'язку із цим, в мережі Інтернет злочинець ототожнюється із іншою, неналежною йому IP-адресою, а справжні дані користувача, у тому числі справжня IP-адреса, інформація, яке передається та отримується, шифруються за допомогою засобів криптографії, що унеможливлює їх зчитування.

2. Застосування відкритих проксі-серверів. Проксі-сервер (від англ. proxy – «представник, уповноважена особа») – це проміжний сервер (комплекс програм) в комп'ютерних мережах, що виконує роль посередника між користувачем і цільовим сервером. Відкритий проксі-сервер представляє собою сервер, що обробляє запити від будь-яких IP-адрес в Інтернеті.

Відкритий проксі-сервер дозволяє практично будь-якому вузлу мережі звертатися через себе до інших вузлів мережі. При цьому, коли говорять про відкриті проксі-сервери, то часто мають на увазі анонімні відкриті проксі-сервери, які приховують реальні IP-адреси клієнтів і тим самим надають можливість анонімно користуватися послугами мережі Інтернет (відвідувати сайти, брати участь у форумах) [7, с. 248].

Для використання відкритого проксі-серверу користувач заходить на веб-сайт, що надає послугу такого серверу, вводить в адресний рядок адресу веб-сторінки, яку користувач бажає відвідати анонімно. Проксі-сервер завантажує цю сторінку собі, обробляє її та передає користувачеві від свого імені. Це представляє певну проблему, оскільки подібна анонімність може дозволити безкарно порушувати закон і умови надання послуг в мережі.

3. Застосування мережі TOR. TOR (від англ. – The Onion Router) – це система, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від прослуховування. TOR розглядається як анонімна мережа віртуальних тунелів, що здійснює передачу даних в зашифрованому вигляді [7, с. 248]. Фактично TOR представляє собою систему проксі-серверів, які захищені багаторівневим шифруванням. Усі проксі-сервери, які беруть участь в процесі передачі даних, вибираються випадково, а тому відстежити реального абонента майже неможливо.

За допомогою TOR користувачі можуть зберігати анонімність при відвідуванні веб-сайтів, публікації матеріалів, відправці повідомлень та інше. У зв'язку із цим, TOR активно використовується в авторитарних державах, де публічна критика переслідується з боку влади. Крім того, TOR використовується приватними особами для забезпечення таємниці свого приватного життя, а корпорації та організації – для забезпечення комерційної таємниці та інших даних, що можуть зашкодити охоронюваним інтересам.

В цілому, TOR розглядається як наукове досягнення с технічної точки зору, що забезпечує високу конфіденційність абонентів мережі, та, одночасно, як правова цінність та інструмент демократичного суспільства, адже TOR дозволяє вільно висловлювати свої думки, передавати важливу для суспільства інформацію без страху нести відповідальність за свої дії.

Разом з тим, використовуючи переваги мережі TOR, злочинці використовують його для розповсюдження порнографічних матеріалів, створення онлайн-майданчиків для продажу наркотичних засобів, порушення авторських та суміжних прав, розповсюджуючи викрадені наукові, художні, музикальні твори, кінофільми тощо для відкритого доступу, що, в свою чергу, значно ускладнює або унеможливлює встановлення особистості таких злочинців. Крім того, складнощі досудового розслідування полягають у тому, що фізичні носії (сервери) забороненої до розповсюдження інформації знаходяться поза межами території України, що значно ускладнює процес ідентифікації особистості злочинця або робить його неможливим.

Висновки

Ідентифікація особистості злочинця, який вчинив кримінальне правопорушення в мережі Інтернет, є найголовнішим та найскладнішим завданням, яке стоїть перед слідчим в процесі розслідування злочину. Головними перешкодами є відсутність комплексних наукових досліджень в даному напрямку, недостатність спеціальних знань у слідчих та працівників оперативних підрозділів, а також дії самих злочинців, які приховують віртуальні сліди та використовують засоби криптографії.

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.

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.

Перспективами подальших розробок у даному напрямку є дослідження способів ідентифікації злочинця, які використовують засоби анонімізації даних в мережі Інтернет, вивчення мережевих ідентифікаторів, які сприяють встановленню криміналістично значимої інформації, аналіз останніх наукових та технічних досягнень, спрямованих на ідентифікацію винних осіб, а також подальший аналіз способів дослідження особистості злочинця на підставі віртуальних слідів, залишених в глобальній мережі.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Закон України від 13.04.2012 № 4651-VI в ред. від 14.04.2017 р. // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/4651-17.

2. 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.

3. 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.

4. Манжай О.В., Осятинська І.А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами / О.В. Манжай, І.А. Осятинська // Актуальні питання розслідування кіберзлочинів. Матеріали міжнародної науково-практичної конференції. – Х., 2013 р. – С. 256 – 258.

5. Поджаренко К.Є. Особливості проведення огляду місця події по справах про злочинні порушення прав інтелектуальної власності / К.Є. Поджаренко // Право і суспільство*, 2009. – № 1. – С. 135-138.

6. Поджаренко К.Є. Криміналістичне забезпечення розкриття і розслідування злочинних порушень прав інтелектуальної власності: автореф. дис. ... канд. юрид. наук : 12.00.09 / К.Є. Поджаренко; Київ. нац. ун-т ім. Т. Шевченка. – Київ, 2009. – 18 с.

7. Струков В.М., Торяник В.В. Актуальні технології протидії розслідуванню мережевих кіберзлочинів / В.М. Струков, В.В. Торяник // Актуальні питання розслідування кіберзлочинів. Матеріали міжнародної науково-практичної конференції. – Х., 2013 р. – С. 247 – 249.

8. Шепітько В.Ю., В.В. Білоус. Роль сучасних інформаційних технологій у встановленні особи злочинця / В.Ю. Шепітько, В.В. Білоус // [Електронний ресурс]. – Режим доступу: http://dspace.nlu.edu.ua/bitstream/123456789/7394/1/Shepitko_Bilous_5_11.pdf.

9. Браузери можуть ідентифікувати користувачів Інтернету // [Електронний ресурс]. – Режим доступу: http://ipress.ua/news/istorii_brauzeriv_mozhut_identyfikuvaty_korystuvachiv_internetu_5606.html.

В статье исследованы способы установления личности преступников, совершающих уголовные правонарушения в сети Интернет, возможности использования сетевых идентификаторов и других виртуальных следов в процессе установления субъектов преступления. Проанализированы роль и значение информационных технологий и социальных сетей в процессе расследования уголовных правонарушений. Исследованы наиболее оптимальные и рациональные приемы, которые составляют комплекс действий следователя и оперативных подразделений, направленных на установление лиц, совершивших преступления в сети Интернет. Определены основные проблемы и сложности, которые препятствуют эффективному установлению субъектов преступления в глобальной сети.

Ключевые слова: субъект преступления, установления преступника, Интернет, информационные технологии, идентификация преступника.

The article explores ways of identifying the criminals who commit criminal offenses in the Internet, the use of network identifiers and other virtual traces in the process of identifying the subjects of crimes. The role and importance of information technologies and social networks in the process of investigating the criminal offenses are analyzed. The article examines the most optimal and rational methods that constitute a set of actions of the investigator and operational units aimed at identifying subjects who commit crimes in the Internet. The main problems and difficulties which hinder the effective establishment of crime subjects in the global network are identified.

Key words: subject of the crime, the Internet, information technology, offender identification, crime investigation.