допитів має певну специфіку: 1) допит потерпілого обумовлюється активною роллю останнього у розслідуваній події та зацікавленістю у поверненні матеріальних збитків, з чим пов'язане нерідке приховування певних фактів, які не є для нього вигідними; 2) допит свідків визначається їх відношенням до розслідуваної події та їх залежністю від тих чи інших осіб; 3) тактичний вплив слідчого щодо підозрюваного зумовлюється процесуальним положенням останнього та незацікавленістю у встановленні об'єктивної істини через перспективи кримінальної відповідальності.

Різноманітність способів вчинення злочинів у сфері приватного житла та використання низки документів зумовлює потребу у призначенні почеркознавчої та техніко-криміналістичної експертизи документів з метою встановлення ознак підробки, ідентифікації особи за ознаками почерку та підпису тощо.

Ключові слова: початковий етап, розслідування, шахрайство, обман, зловживання довірою, житло.
Ключевые слова: начальный этап, расследование, мошенничество, обман, злоупотребление доверием, жилье.
Key words: initial stage, investigation, fraud, deception, abuse of trust, housing.

ХИЖНЯК ЄВГЕН СЕРГІЙОВИЧ

Національний університет «Одеська юридична академія»,
декан факультету адвокатури, доцент кафедри криміналістики,
кандидат юридичних наук, адвокат

ОСОБЛИВОСТІ ІДЕНТИФІКАЦІЇ ОСОБИ ЗЛОЧИНЦЯ ЗА ДОПОМОГОЮ IP-АДРЕСИ

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.

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 кон-

тенту 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'єкта прогнозування, його майбутньої поведінки [1, 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.

Інформація, що є доступною у мережі Інтернет, у тому числі й та, що міститься на веб-сайтах, 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 складається з 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 електроннообчислювальної машини, з якої було здійснено реєстрацію веб-сайту, IP-адресу електроннообчислювальної машини, з якої здійснювалось управління веб-сайтом та наповнення веб-сайту забороненим контентом [2, с. 221].

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) [3, с. 248].

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 [3, 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.

Таким чином, основним способом ідентифікації особи злочинця є встановлення його особистості за допомогою IP-адреси домену сайту, на якому розміщено заборонену 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.

Список використаної літератури:

1. Шепітько В.Ю., Білоус В.В. 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.
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. – С. 218-222.
3. 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. – С. 247-249.

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

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

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

ЦЕХАН ДМИТРО МИКОЛАЙОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри криміналістики, кандидат юридичних наук, доцент

ТЕОРЕТИЧНА МОДЕЛЬ ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ ЗЛОЧИННОСТІ У МІСЦЯХ ПОЗБАВЛЕННЯ ВОЛІ

Аналізуючи відповідні структурні рівні оперативно-розшукової протидії злочинності у місцях позбавлення волі як окремий структурний блок може бути виокремлений теоретичний рівень такої протидії.

Оперативно-розшукову протидії злочинності у місцях позбавлення волі можна визначити як відповідну теоретичну модель у межах якої обґрунтовуються оптимальні форми впливу на пенітенціарну злочинність на конкретному етапі історичного розвитку суспільства, правової системи та держави. У даному випадку як відповідна теоретична модель оперативно-розшукова протидія злочинності у місцях позбавлення волі інтегрує теоретичні напрацювання дослідників щодо цієї проблематики, результати діяльності суб'єктів, уповноважених на формування та затвердження загальнодержавних концепцій та стратегій протидії злочинності та функціонування державних інституцій, які здійснюють таку протидію, результати діяльності уповноважених