

УДК 343.98

ОСОБЛИВОСТІ СЛІДОВОЇ КАРТИНИ ШАХРАЙСТВ, ЩО ВЧИНЯЮТЬСЯ В МЕРЕЖІ ІНТЕРНЕТ

Романенко Т.В.

Київський національний університет імені Тараса Шевченка

У статті визначаються поняття та види слідів шахрайств, що вчиняються в мережі Інтернет. Приділено увагу нетрадиційним слідам, які утворюються в результаті вчинення цього злочину. Розглядаються особливості утворення слідів інтернет-шахрайства. До елементів «слідової картини» віднесено інформацію про місце та час вчинення злочину. Запропоновано використати наукове дослідження при розробці криміналістичної методики розслідування шахрайств, що вчиняються в мережі Інтернет.

Ключові слова: шахрайство, інтернет-шахрайство, кібершахрайство, сліди, віртуальні сліди, інформаційні сліди.

Постановка проблеми. Стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет та його використання в різних сферах суспільного життя стає умовою для вчинення злочинів, які несуть загрозу економічному та соціальному життю як громадянина, так і держави. Україна вже давно асоціюється

у світі з місцем, де процвітає кіберзлочинність. Ще 2012 року американський спеціалізований журнал Computerworld присвятив велику статтю Україні, називаючи країну «раєм для хакерів», адже українські кіберзлочинці добре відомі у світі і несуть загрозу для багатьох країн. Сьогодні почалася реформа правоохоронних органів і створювана нині кіберполіція буде спеце-

партаментом, який прийде на зміну нинішньому управлінню по боротьбі з кіберзлочинністю. Для цього потрібно постійно удосконалювати криміналістичні методи розслідування злочинів та віддавати належне окремим елементам криміналістичної характеристики. У зв'язку з цим аналіз елементів слідової картини має важливе криміналістичне значення під час виявлення, вилучення, фіксації та дослідження слідів злочинного діяння у процесі розслідування злочинів, що вчиняються в мережі Інтернет.

Аналіз останніх досліджень і публікацій. Проблеми вивчення типових слідів під час розслідування шахрайських дій, що вчиняються в мережі Інтернет все частіше стають предметом дослідження криміналістів. Цій проблемі присвячені роботи таких вчених, як Мещеряков В. А., Мусієнко О. Л., Паламарчук Л. П., Постіл Н. С., Семенов Г. В., Федотов М. М. та інші.

Виділення не вирішених раніше частин загальної проблеми. Більшість науковців у своїх працях акцентують увагу на слідах шахрайств, що вчиняються в побутовій сфері. Питання вивчення слідів, які залишаються при вчиненні шахрайств в мережі Інтернет та специфіка їх утворення на сьогоднішній день не досліджена в повному обсязі.

Мета статті. Головною метою цієї роботи є дослідження слідової картини шахрайських дій, що вчиняються в мережі Інтернет.

Виклад основного матеріалу. Вчинення багатьох злочинів супроводжується певними змінами у навколишньому середовищі. Такі зміни прийнято називати слідами злочину. Слід являє собою відображення злочинних дій або окремих елементів злочинної діяльності. У криміналістичному розумінні цінність слідів зумовлена існуючою залежністю між злочином та його відображенням в навколишньому середовищі (слідами). У криміналістиці сліди розуміють у широкому та вузькому значенні. У широкому розумінні сліди – це результат будь-якої матеріальної зміни первинної обстановки внаслідок вчинення злочину: матеріально-фіксовані зміни одного об'єкта на інший; поява чи зникнення тих чи інших предметів, порушення первинного стану, місцезнаходження, стану різних об'єктів (наприклад, загублені злочинцем на місці події власні речі, скалки розбитого віконного скла). А сліди у вузькому розумінні, це – матеріально-фіксовані відображення зовнішньої будови одного об'єкта на іншому (сліди-відображення). Сліди-відображення виникають внаслідок взаємодії двох об'єктів і мають достатньо широке розповсюдження: це сліди рук людини, ніг, взуття, зубів, транспортних засобів, знарядь та інструментів тощо.

Слідова картина є важливим елементом криміналістичної характеристики шахрайств, які вчиняються в мережі Інтернет. Як відомо, слідова картина відображає особливості способу, а також ознаки інших елементів структури злочинної діяльності. Інтернет-шахрайство є особливим видом кіберзлочинів та вчиняється шляхом обману або зловживання довірою [1]. Правильна криміналістична оцінка слідів даного злочину дасть змогу співробітникам органів внутрішніх справ створити основу для найбільш швидкого розпізнання в первинних слідчих даних по кримінальному про-

вадженню того чи іншого характерного способу вчинення розслідуваного злочину навіть за окремими характерними йому ознаками. Тому слід погодитись із Мусієнком О. Л., який вважає що типові сліди як елемент криміналістичної характеристики шахрайства, зокрема і в мережі Інтернет, дають змогу сформувати уявлення про спосіб вчинення злочину, предмет злочинного посягання, особу злочинця, відображають обстановку, в якій вчинявся злочин, тобто вони є носіями різнобічної інформації, до якої може звертатися слідчий при розслідуванні конкретного злочину [2, с. 96]. А от Л. П. Паламарчук слушно зазначає, що через специфіку злочину сліди рідко виявляються у змінах зовнішнього середовища [3, с. 38].

У криміналістиці прийнято виділяти матеріальні та ідеальні сліди злочину, але все частіше суб'єктам криміналістичної діяльності доводиться виявляти, вилучати, фіксувати та досліджувати не тільки традиційні сліди злочину, але й нові різновиди відображень події злочину у навколишньому середовищі, які на сьогоднішній день вже не належать до тієї чи іншої з перелічених груп, а утворюють нову групу слідів, які називають інформаційними, або ж віртуальними. Тому проаналізуємо окремо та більш детально кожну групу слідів, які можна виявити під час проведення слідчих (розшукових) дій та дослідимо механізм їх утворення.

При визначенні матеріальних слідів інтернет-шахрайства необхідно застосувати традиційний поділ таких слідів на сліди-відображення, сліди-предмети та сліди-речовини.

Сліди-відображення класифікують за: характером змін і виділяють структурні та зовнішні файлові сліди; розміщенням поділяють на локальні та мережні файлові сліди; процесом обробки команд поділяють на постійні в часі та тимчасові файлові сліди.

Сліди-предмети класифікують таким чином: змінні диски, пристрої дистанційного зняття інформації, USB-флеш-накопичувачі, мобільні телефони, планшети, банкомати, пластикові картки, документи на електронних та паперових носіях, тощо.

Сліди-речовини можуть проявлятися у вигляді витратних матеріалів, зокрема це порошки, фарби. Але також сліди-речовини можуть бути біологічного походження, які злочинець випадково залишив на місці вчинення злочину, на знаряддях вчинення злочину чи певному предметі злочину.

Наприклад, при розслідуванні шахрайств з банківськими картками до матеріальних слідів відносять безпосередньо виконані записи шахраєм номерів телефонів, карток потерпілих, а також створення злочинцем нових карток для переміщення на них коштів отриманих злочинним шляхом. Сліди також можуть залишатися на технічних засобах (сліди від пальців рук, мікрочастинки на клавіатурі, тощо), а також на магнітних носіях.

Окрему групу складають ідеальні сліди. Це сліди, що містяться в пам'яті людини. На думку вчених, ідеальні сліди – це відображення події або її елементів у свідомості людини, уявний образ сприйнятого. Р. С. Белкін називає такі сліди ідеальними або образом, тобто слідом у свідомості людини, уявним «відбитком» події в

пам'яті людей. Такий слід може містити інформацію не лише про подію або факт, але й про пов'язані з ними обставини, про особу злочинця, про взаємозв'язок з потерпілим тощо. Носіями ідеальних слідів можуть бути не лише очевидець і свідок, але й інші особи (потерпілий, підозрюваний) [4, с. 14-15]. При розслідуванні шахрайств, що вчиняються в мережі Інтернет ідеальними слідами можуть бути певні відображення, що залишаються в пам'яті людини, частіше після телефонних розмов із шахраєм.

До нетрадиційних слідів відносяться інформаційні, або їх ще називають віртуальними. Інформаційними їх слід називати тому, що вони утворюються в результаті впливу на комп'ютерну інформацію шляхом доступу до неї і являють собою будь-які зміни комп'ютерної інформації, пов'язані з подією злочину, у зв'язку із застосуванням інформаційних технологій [5, с. 139].

Специфіка механізму утворення інформаційних слідів визначається кіберпростором, тобто слідоутворюючим об'єктом, яким виступає програмно-технічний засіб, а слідоприймаючим об'єктом – комп'ютерною інформацією. Існує порядок зчитування інформації з її носія, а саме: фізичні сигнали (фізичний рівень) – цифрова форма (логічний рівень) – текст, графіка, звук (семантичний рівень); під час запису інформації на її носій – у зворотному напрямі. Зміни на будь-якому рівні, що відбуваються в результаті відповідного впливу (фізичний – за допомогою технічних пристроїв; програмний без участі людини; вплив людини на зміст інформації за допомогою програмних засобів) відразу ж призводять до змін на інших рівнях. На слідоприймаючому об'єкті відображається не форма слідоутворюючого об'єкта, а їх властивості, оскільки програмно-технічні засоби не мають зовнішньої форми.

Зазначимо, В. А. Мещеряков розглядає віртуальні сліди як зміну стану автоматизованої інформаційної системи (утвореного нею «кібернетичного простору»), пов'язаної з подією злочину і зафіксованою у вигляді комп'ютерної інформації (тобто інформації у вигляді, придатному для машинної обробки) на матеріальному носії, у тому числі і на електромагнітному полі. А на думку Г. В. Семенова, віртуальні сліди – це комп'ютерна інформація на матеріальних носіях комп'ютерної техніки (програмне забезпечення, за допомогою якого здійснюється сканування, декодування, запис і зберігання необхідних даних, підробка документів і інші супутні злочини, продукти застосування вказаних спеціальних програм, повідомлення телекомунікаційних сервісів (SMS, EMS, MMS), персональні дані абонента і тому подібне) [6, с. 222-223].

На нашу думку, інформаційними слідами є певні відображення, які утворилися внаслідок впливу на комп'ютерну інформацію шляхом доступу через глобальну мережу Інтернет, були пов'язаними зі зміною інформації та залишилися на магнітних носіях.

Схема всіх шахрайств в мережі Інтернет зазвичай складається з таких етапів: розміщення (розсилка) інформації, реклами; взаємодія (спілкування) з жертвою як по телефону, так і шляхом інтернет чи СМС переписки; отримання грошових коштів шляхом переказу.

Всі три етапи передбачають залишення великої кількості слідів технічного характеру. Хоча шахраї, зазвичай, намагаються здійснювати певні дії для своєї анонімності. Під час отримання грошей шахраїв крім анонімності рятує ще й швидкість, адже переказ отриманих коштів між різними платіжними системами здійснюється досить швидко, але вимагає багато часу для відстеження [7, с. 199].

При розміщенні шахраями підробленого інтернет-магазину можна розраховувати на виявлення таких слідів: реєстраційні дані на доменне ім'я; логи від взаємодії з реєстратором доменних імен; сліди від проведення платежу цього реєстратора; сліди при налаштуванні DNS-сервера, що підтримує домен шахраїв; сліди від взаємодії з хостинг-провайдером, у якого розміщений веб-сайт: замовлення, оплата, настройка, заливши контенту; сліди від рекламування веб-сайта: взаємодія з рекламними майданчиками, системами банерообміну, розсилка спаму; сліди від відстеження активності користувачів на сайті, тощо.

При взаємодії з жертвами обману шахраї залишають сліди при прийомі замовлень – по електронній пошті, через СМС повідомлення, через ICQ, або веб-форму; від листування з потенційними жертвами.

При отриманні грошей шахраї залишають сліди при здійсненні введення грошей в платіжну систему (реквізити, які вказуються жертві); при переказі грошей між рахунками, які контролюються шахраями; сліди при виведенні грошей; від дистанційного керування шахраями своїми рахунками, їх відкриття і закриття; від взаємодії шахраїв з посередниками з відмивання і переведення грошей у готівку.

Варто зазначити, що до «слідової картини» окрім інформації про сліди містить також відомості про місце та час вчинення злочину [3, с. 42]. Місце безпосереднього вчинення протиправного діяння (місце знаходження злочинця, засобів вчинення злочину) не співпадає з місцем знаходження потерпілого і настання наслідків злочину, що пов'язано з використанням електронних технічних засобів та мережі Інтернет. Зазвичай місцем вчинення інтернет-шахрайства можуть бути місця проживання, роботи або навчання злочинця. Тобто злочинець має можливість заволодіти майном потерпілого використовуючи лише технічні засоби, не маючи з ним особистого контакту, хоча, можуть здійснюватись телефонні дзвінки до потерпілого. Тому, можна відзначити, що місцезнаходження електронного технічного засобу і є місцем вчинення злочину. Разом з тим особливістю злочинів даної групи є те, що вони можуть бути вчинені в різноманітних сферах суспільного життя, зокрема, у побуті, підприємницькій діяльності тощо, але обстановка вчинення шахрайства характеризується на частіше відсутністю свідків. Правоохоронній практиці також відомі факти, що шахрайства в мережі Інтернет та по телефону вчиняються ув'язненими особами у місцях позбавлення волі, які відбувають покарання за різні види злочинів по всій території України.

Час вчинення шахрайств з використання електронних технологій характеризується досить тривалою подією у часі. Злочинцю потрібен час для здійснення технічної підготовки до

злочину, а також в деяких випадках отримати необхідну інформацію про потерпілого. Інформація отримується від потерпілої особи переважно вранці чи вдень, рідше – у вечірній час. Поширюється практика заволодіння коштами шляхом обману телефонними дзвінками в нічний час, коли зловмисники повідомляють про нещасні випадки, про участь родича у ДТП, затримання родича поліцією та просять через інтернет-банкінг перечислити гроші.

Висновки і пропозиції. Таким чином, на основі вище викладеного можна зробити висновки, що слідова картина шахрайств що вчиняються в мережі Інтернет є специфічною, адже злочинець підбирає всі можливі засоби, які можна використати в електронному середовищі.

Проаналізувавши механізм утворення слідів, що має важливе криміналістичне значення при

розслідуванні шахрайств, що вчиняються в мережі Інтернет, встановлено що вони можуть бути як традиційними – ідеальні та матеріальні, так і нетрадиційними – інформаційні, або їх ще називають віртуальними. Для виявлення, фіксації, вилучення та дослідження слідів цього злочину необхідні як криміналістичні знання, так і спеціальні знання в сфері використання комп'ютерних технологій.

Дослідження слідів шахрайських дій в мережі Інтернет є важливим елементом криміналістичної характеристики та допоможе створюванам нині підрозділам кіберполіції в швидкому виявленні, розслідуванні та розкритті злочинів. Дана проблематика є актуальною відповідно до реалій сьогодення та має перспективи подальшого наукового дослідження в майбутньому, зокрема, при розробці криміналістичної методики розслідування шахрайств, що вчиняються в мережі Інтернет.

Список літератури:

1. Конвенція про кіберзлочинність: від 23 листоп. 2001 р. // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575
2. Теоретичні засади розслідування шахрайства в сучасних умовах: монографія / О. Л. Мусієнко; за ред. проф. В. Ю. Шепітька. – Харків: Право, 2009. – 168 с.
3. Паламарчук Л. П. Розслідування злочинів у сфері використання комп'ютерних технологій. Монографія – К., 2007. – 144 с.
4. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації): монографія / Д. В. Затенацький; за ред. В. Ю. Шепітька. – Харків: Право, 2010. – 160 с.
5. Постіл Н. С. Класифікація слідів комп'ютерних злочинів / Н. С. Постіл, П. В. Цимбал // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения: материалы международной научно-практической конференции (Донецк, 18-19 мая 2006 г.). – Донецк: ДЮИ ЛГУВД, 2007. – С. 138-140.
6. Дослідження віртуальних слідів – перспективний напрямок криміналістичного слідознавства / В. Д. Басай, С. В. Томин // Актуальні проблеми держави і права. – 2008. – Вип. 44. – С. 220-223.
7. Федотов Н. Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

Романенко Т.В.

Киевский национальный университет имени Тараса Шевченко

ОСОБЕННОСТИ СЛЕДОВОЙ КАРТИНЫ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ В СЕТИ ИНТЕРНЕТ

Аннотация

В статье определяются понятия и виды следов мошенничеств, совершаемых в сети Интернет. Уделено внимание нетрадиционным следам, которые образуются в результате совершения этого преступления. Рассматриваются особенности образования следов интернет-мошенничества. К элементам «следовой картины» относится информация о месте и времени совершения преступления. Предложено использовать научное исследование при разработке криминалистической методики расследования мошенничеств, совершаемых в сети Интернет.

Ключевые слова: мошенничество, интернет-мошенничество, кибермошенничество, следы, виртуальные следы, информационные следы.

Romanenko T.V.

Taras Shevchenko National University of Kyiv

FEATURES PICTURES TRACE FRAUD COMMITTED ON THE INTERNET

Summary

The article defined the concept and types of tracks frauds committed on the Internet. Attention is paid to non-traditional tracks that are formed as a result of the commission of the crime. The features of formation of traces of Internet fraud. The elements of «trace pattern» include information about the place and time of the offense. A use scientific research in the development of forensic investigation techniques frauds committed on the Internet.

Keywords: fraud, Internet fraud, cyber fraud, traces, virtual traces, information traces.