Чучко Сергій Віталійович
ад'юнкт кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ

ВІРТУАЛЬНІ (КОМП'ЮТЕРНІ) СЛІДИ ШАХРАЙСТВА, ПОВ'ЯЗАНОГО ІЗ ТОРГІВЛЕЮ ТОВАРАМИ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Згідно традиційної думки, сліди у широкому розумінні розглядаються як будь-які зміни в середовищі, що виникають внаслідок вчинення злочинної діяльності. При чому, у класичному варіанті до недавнього часу всі сліди поділялися на дві групи: матеріальні та ідеальні.

В контексті сказаного не можна не визнати той факт, що за останні десятиріччя у криміналістиці з'явився третій вид слідів, який не відноситься ані до матеріальних, ані до ідеальних слідів. Аналіз криміналістичної літератури показав, що ця група слідів має різні назви: «комп'ютерні сліди», «віртуальні сліди», «інформаційні сліди», «електронні сліди» та ін. Вважаємо не принциповим застосування будь-якого із вказаних термінів, якщо вони повністю відображають сутність злочинів, вчинених внаслідок використання комп'ютерної мережі.

Віртуальні сліди розглядаються як будь-яка зміна стану автоматизованої інформаційної системи (утвореного нею «кібернетичного простору»), пов'язана з подією злочину та зафіксована у вигляді комп'ютерної інформації на матеріальному носії, у тому числі й на електромагнітному полі [1, с. 21].

В криміналістичній літературі можна виділити різні підходи до класифікації віртуальних (віртуальних) слідів.

Так, Я. Найдьон поділяє віртуальні сліди на 4 групи:

1) за походженням: електронна інформація, створена ЕОМ у процесі своєї роботи; електронна інформація, створена в процесі діяльності людини; похідна електронна інформація, створена комп'ютером на основі введених даних користувачем, або навпаки, інформація, створена з даних, згенерованих комп'ютерною системою;

2) за формою подання: інформація, доступна для сприйняття людиною; інформація, представлена у вигляді машинного коду;

3) за місцем зберігання: дані, що зберігаються в комп'ютерних системах; дані, скопійовані або переміщені користувачем на електронні носії (жорсткі диски, компакт-диски, накопичувачі); паперові копії (копії листування, скріншоти та ін.);

4) за формою: вихідні дані (інформація, введена людиною); бази даних; коди шифрування; програмне забезпечення різних видів; комп'ютерні системи [2, с. 305].

Деякі складові до такої класифікації додав Д. В. Бахтеєв. Вчений здійснив криміналістичну класифікацію цифрової доказової інформації за наступними критеріями:

- за формою носія: цифрові (віртуальні) сліди, розташовані на оптичних, напівпровідникових і магнітних носіях;

- за способом доступу: доступ до яких здійснюється локально або віддалено,

розміщені у відкритому доступі і захищені сліди;

- за місцем зберігання: у володінні злочинця (персональний комп'ютер, жорсткий диск, мобільний телефон), на пристроях потерпілого, свідка, сторонніх осіб та цифрові сліди, які одночасно зберігаються на пристроях усіх указаних осіб і в мережі Інтернет;

- за типом пристрою, на якому зберігаються цифрові сліди: стаціонарні і мобільні;

- за цільовим призначенням: шкідливі програми і корисні програми (додатки з різноманітними функціями, необхідні для здійснення тактичних операцій або дій, що допомагають у повсякденній діяльності, у побуті, роботі тощо) [3, с. 19].

Є. С. Хижняк звернув увагу, що А. Волєводза в основу класифікації віртуальних слідів взагалі обрав один єдиний критерій – фізичний носій «віртуального сліду». Зокрема: 1) сліди на жорсткому диску (вінчестері); 2) сліди на магнітній стрічці, оптичному диску (CD, DVD); 3) сліди в оперативних запам'ятовуючих пристроях (ОЗУ) ЕОМ; 4) сліди в ОЗУ периферійних пристроїв (лазерного принтера, наприклад); 5) сліди в ОЗУ комп'ютерних пристроїв зв'язку і мережевих пристроїв; 6) сліди у провідних, радіооптичних та інших електромагнітних системах і мережах зв'язку [4, с. 305]. Деякі вчені в основу класифікації покладають процесуальне положення суб'єкта: 1) сліди на комп'ютері злочинця; 2) сліди на комп'ютері жертви [5, с. 56]. Хоча, як на наш погляд, така класифікація є дещо узагальненою і не охоплює інші складові, наприклад, сліди у провідних та інших електромагнітних системах і мережах зв'язку та ін.

Аналізуючи наведені погляди на класифікацію можна побачити, що здебільшого вчені покладають в основу класифікації віртуальних (комп'ютерних) слідів такі критерії, як: місце зберігання, форма, походження та призначення.

Для більш повного розуміння суті шахрайських дій, вчинених при здійсненні цивільно-правових угод через мережу Інтернет, та слідів, які залишаються внаслідок таких дій, необхідно проаналізувати особливості діяльності сайтів і мобільних додатків, які слугують для спілкування між шахраєм та потерпілим.

Як повідомляють дослідники у напряму підвищення безпеки проведення фінансових операцій в мережі Інтернет, алгоритм фінансових операцій в мережі здебільшого відбувається у такий спосіб. Сайти надають можливість своїм користувачам виставляти лоти на продаж та вести торги за вже виставлені лоти. Для цього всі користувачі повинні: 1) зареєструватися на сайті – для кожного окремого інтернет порталу встановлюється адміністрацією порталу; 2) підтвердити реєстрацію; 3) виставити лот, встановивши його початкову вартість. Сайт виступає в якості посередника між продавцем та покупцем, надаючи «середовище» для проведення торгів. На більшості таких сайтах є можливість: − продивлятись фотографії лотів, їх відео-записи; − читати відгуки та коментарі стосовно певних лотів, осіб, що виставляють лоти (продавців) та осіб, що беруть участь в аукціоні як покупці, а також вести переписку між користувачами для обговорення деталей угоди (форма відправки товару, терміни відправки, форма сплати тощо). Відповідно до загально прийнятих правил після закінчення торгів продавець та покупець домовляються про спосіб передачі товару та форму сплати. Для цього покупцю

надсилаються контактні дані продавця [6, с. 153-154].

Отже, хід тривалого спілкування між шахраєм та потерпілим не є прихованим фактом, а може бути відображений у пам'яті електронних пристроїв, за допомогою яких передається інформація. Так, сліди у вигляді віртуальної переписки з питань купівлі-продажу товарів можуть міститися в електронній скриньці, куди надходить інформація від шахрая. Це можуть бути файли і папки зберігання вхідних та вихідних повідомлень електронної пошти, конфігурації поштової програми тощо.

На сторінці веб-сайту також можуть міститися віртуальні сліди (фотографії, відгуки та коментарі стосовно певних лотів, результати переписки між користувачами та продавцями тощо). Сліди можуть міститися й у історії голосових повідомленнях та і відеодзвінках (відеододатки Skype, Google Hangouts, Zoom тощо). Втім, найцінніша інформація криється у доменній адресі (Ip), що дозволяє встановити місцезнаходження точки доступу до комп'ютера, з якого здійснювалося спілкування.

Як справедливо наголошує Є. С. Хижняк, домен є головним атрибутом електронного документа, розміщеного в мережі Інтернет. Окрім домену, відіграє важливу роль й URL веб-сторінки, який завжди є індивідуальним, тому використовується як один із способів ідентифікації веб-сторінки, на якому розміщені електронні матеріали, що мають значення для розслідування [4, с. 83].

Як показав аналіз матеріалів кримінальних проваджень, у 62 % випадків шахрай та потерпілий зв'язувалися по телефону з метою обговорювання умов угоди купівлі-продажу товарів. Внаслідок чого в пам'яті мобільного телефону, в пам'яті SIM-карти, в пам'яті флеш-карти залишаються віртуальні сліди. Це можуть бути: сліди з'єднання, смс повідомлення, електронно-цифрові сліди у вигляді фотографій товару тощо.

Оскільки здебільшого шахраї і потерпілі обирають спосіб електронних розрахунків через електронні платіжні засоби та системи, електронні гаманці, інші види безготівкових розрахунків, у телефоні, в комп'ютері може міститися програмне забезпечення, звідки можна отримати слідову інформацію про проведені банківські операції. За таких обставин банківська карта, рахунок власника картки або рахунок телефонного номера виступають об'єктом слідоутворення.

Використані джерела:

1. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. на соискание учен. степени доктора юрид. наук : спец. 12.00.09. Воронеж, 2001. 39 с.

2. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємство,господарство і право*. 5/2019. С. 304-307.

3. Бахтеев Д.В. Криминалистическая классификация цифровой доказательственной информации. Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сб. статей Международ. науч.- практ. конф. М.: Академия управления МВД России, 2018. С. 44–55.

4. Хижняк Є. С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права*. 2017. С. 159-166.

5. Мочагин П.В. Виртуально-информационный процесс отражения следообразований как новое направление в криминалистике. *Вестник криминалистики*, 2013. № 3. С. 51–57.

6. Бойко А.О., Чещевий Є.І., Безрук В.В. Алгоритмізація процесу підвищення безпеки проведення фінансових операцій в мережі Інернет. *Вісник СумДУ. Серія "Економіка",* № 3' 2017. С. 152-158.

Пекарський С.П. доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 1
Донецького юридичного інституту МВС України, кандидат юридичних наук

ВИКОРИСТАННЯ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОПЕРАТИВНОГО ПРИЗНАЧЕННЯ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС

Стаття 25 Закону України «Про Національну поліцію» [1] визначає повноваження поліції у сфері інформаційно-аналітичного забезпечення. Відповідно до положень даної статті поліція в рамках інформаційно-аналітичної діяльності: формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

На підставі зазначеного та відповідно до предмету даного дослідження проведемо аналіз використання автоматизованої інформаційної системи оперативного призначення єдиної інформаційної системи МВС. Так використання інформаційних технологій в діяльності Національної поліції має правову регламентацію. Зокрема, Законами України: «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», тощо визначені повноваження кримінальної поліції щодо використання інформаційних технологій. Окрім того, Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС, яке затверджено наказом МВС України від 20.10.2017 № 870 [2] визначає основні завдання, функції,