УДК 343.98

Г. К. Авдєєва, *доцент кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук, старший науковий співробітник, e-mail: gkavdeeva@gmail.com*

СУТНІСТЬ ЦИФРОВИХ СЛІДІВ У КРИМІНАЛІСТИЦІ

Цифрові пристрої і технології широко використовуються в усіх сферах діяльності людини, що слугує підґрунтям для поширення нових видів злочинів із їх використанням. Прикладами таких злочинів слугують неправомірні зовнішні втручання в роботу енергетичних і транспортних структур, банків,

окремих державних та приватних установ (кібератаки)[1]. Жертвами шахрайства в мережі Інтернет стають і фізичні особи[2].

Правопорушники використовують цифрові пристрої та телекомунікаційні мережі для збирання й крадіжки інформації про потенційну жертву злочину, для комунікації членів злочинного угруповання під час підготовки та вчинення злочину та ін. На сайті Національної поліції України навіть розміщено рекомендації щодо фіксації цифрових слідів, які в подальшому можуть бути використані як докази при розслідуванні інтернет-шахрайства[3]. Тому проблеми дослідження цифрових слідів у криміналістиці на сьогодні є актуальними.

Питанням дослідження проблем боротьби зі злочинами, які вчиняються з використанням цифрових пристроїв, учені-криміналісти приділяють значну увагу. Науковці зазначають, що традиційний розподіл слідів у криміналістиці на сліди в широкому сенсі (результат будь-якої матеріальної зміни первинної обстановки внаслідок учинення злочину) та у вузькому (відображення під час учинення злочину на одному з об'єктів взаємодії слідів зовнішньої будови іншого об'єкта) практично не охоплює злочини, що вчиняються з використанням цифрових засобів. В окремих працях зазначено, що на сучасному етапі розвитку криміналістики як сліди розглядаються й електронні (цифрові)[4]. Учені дискутують не лише щодо сутності цифрових слідів злочинів, а й стосовно їх найменування (комп'ютерні сліди, віртуальні сліди, електронно-цифрові, інформаційні, комп'ютерно-технічні, електронні, цифрові сліди тощо)[5].

Цифрові сліди утворюються цифровими пристроями (англ. digital device) – технічними пристроями або пристосуваннями, призначеними для отримання й оброблення інформації в цифровій формі з використанням цифрових технологій. Технічно цифрові пристрої можуть бути виконані на основі електромагнітних реле, на діодах і транзисторах, мікросхемах та ін. Найбільш поширеними є цифрові пристрої на мікросхемах (телефони, смартфони, комп'ютери, портативні пристрої геолокації, цифрові фотокамери, відеореєстратори, веб-камери, мережеві маршрутизатори, платіжні системи та ін.). Такі пристрої все частіше використовуються злочинцями і, як наслідок, цифрові сліди неправомірних дій залишаються в інформаційному просторі.

Цифровий слід має певну систему ознак у вигляді окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох носіях цифрової інформації. Носії таких слідів можуть бути одночасно підключені до декількох цифрових пристроїв, об'єднаних, наприклад, у телекомунікаційну мережу.

Основою механізму утворення електронних слідів слугують електромагнітні взаємодії двох і більше матеріальних об'єктів, кожен із яких є сукупністю електронного цифрового пристрою (комплексу пристроїв) і системи управління ним (набору програмних продуктів). Об'єкти, які утворюють і сприймають електронні сліди, мають об'єктивну форму існування. Сліди впливу однієї об'єктивної форми існування цифрової інформації на іншу можуть бути виявлені, зафіксовані та вивчені лише за допомогою певних цифрових електронних пристроїв.

Цифровими слідами в криміналістиці є матеріальні невидимі сліди, які містять криміналістично-значущу інформацію (відомості, дані), зафіксовану в цифровій формі на матеріальних носіях і можуть бути виявлені, зафіксовані й досліджені за допомогою певних цифрових пристроїв.

Основними об'єктами, які утворюють і сприймають цифрові сліди, є такі: машинні носії цифрової інформації, інтегральні мікросхеми, мікроконтролери, ЕОМ і їх системи, обладнання телекомунікаційних мереж, цифрові фотокамери та диктофони, пристрої для зчитування інформації з пластикових

---

[1] Кібератаки на Україну коштують мільйони доларів. URL: http://detector.media/infospace/article/122774/2017-02-02-kiberataki-na-ukrainu-koshtuyut-milioni-dolariv-sbu/.

[2] Див., напр.: Вражаюча сума, яку торік вкрали в українців кібершахраї: найпоширеніші злочинні схеми. URL: http://www.expres.ua/news/2017/01/26/225031-vrazhayucha-suma-torik-vkraly-ukrayinciv-kibershahrayi-nayposhyrenishi.

[3] Ви стали жертвою інтернет-шахраїв? *Сайт Національної поліції України*. URL: https://www.npu.gov.ua/uk/publish/article/896018.

[4] Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель [та ін.]; за ред. В. Ю. Шепітька. 5-те вид., перероб. та допов. Київ: Ін Юре, 2016. С. 95–96, Криминалистика: информационные технологии доказывания: учеб. для вузов / под ред. В. Я. Колдина. Москва: Зерцало-М, 2007. С. 164–165. *Авдєєва Г. К, Стороженко С. В.* Електронні сліди: поняття та види. *Вісн. Луган. держ. ун-ту внутр. справ ім. Е. О. Дідоренка*. Сєвєродонецьк, 2017. Вип. № 1 (77). С. 168–174.

[5] Див., напр.: *Веліканов С. В.* До поняття електронного сліду в криміналістиці. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення*: матеріали постійно діючого наук.-практ. семінару, 27 листоп. 2015 р. Харків: Право, 2015. Вип. 7. С. 241–244; *Авдєєва Г. К.* Сліди злочинів у сфері використання електронно-обчислювальних засобів, телекомунікаційних систем і комп'ютерних мереж. *Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції*: монографія / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за заг. ред. В. Ю. Шепітька, В. А. Журавля. Харків: Вид. агенція «Апостіль», 2017. С. 52–62; *Сукманов В. О.* Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений. *Вестн. Калининград. юрид. ин-та МВД России*. С. 104–107; *Вехов В. Б., Смагоринский Б. П., Ковалев С. А.* Электронные следы в системе криминалистики. *Судебная экспертиза*. Волгоград: ВА МВД России, 2016. Вып. 2 (46). С. 10–19, та ін.

банківських карт, мобільні телефони, планшети та ін. Окремі електронні модулі цих засобів дозволяють навіть зафіксувати місце й час перебування пристрою в кожний конкретний момент. Зокрема, за допомогою системи геолокації в режимі реального часу можна визначити точне місцезнаходження конкретного комп'ютера, планшета або мобільного телефону і, відповідно, його власника. Дані геолокації також можуть бути використані для встановлення факту одночасної присутності двох і більше осіб в одному місці, а неодноразова фіксація таких фактів свідчить про їх взаємодію.

Цифрові сліди утворюються внаслідок зовнішнього втручання до комп'ютерних систем із метою знищення або копіювання інформації, модифікації баз даних, блокування роботи системи. Такими слідами є видалення з каталогів імен файлів, видалення або додавання окремих записів, фізичне руйнування або розмагнічування носіїв, перейменування каталогів і файлів, зміна розмірів і вмісту файлів, зміна атрибутів файлів, поява нових каталогів і файлів, зміна інформації про час останнього доступу до інформації, сліди роботи антивірусних і тестових програм та ін. Вони можуть бути виявлені при експертному дослідженні комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду та ін. Сліди неправомірного доступу до інформації містяться в журналах операційних систем і окремих програмних продуктів, які створюють резервні копії файлів і файли-звіти, зберігають інформацію про останні проведені операції та виконані програми, а також містять іншу інформацію, що має значення для розслідування злочину. Аналіз таких цифрових слідів і слідів, які містять відомості щодо стандартної інформації про конфігурацію браузера комп'ютера зловмисника, часто дозволяє ідентифікувати цифровий пристрій, з якого здійснювалося зовнішнє втручання.

Важливу криміналістично-значущу інформацію можна отримати при вивченні даних електронного листування та сервісів обміну SMS (Short Messaging Service – служба коротких повідомлень). В атрибутах файлів електронних листів міститься дата й час відправлення, електронна адреса відправника, найменування й адреса інтернет-провайдера та інша інформація. Найменування й адресу інтернет-провайдера, за допомогою якого правопорушник підключений до мережі Інтернет, можна вільно отримати через спеціальну службу Whois (у мережі Інтернет), зазначивши IP-адресу «атакуючого» комп'ютера. Телефонні дзвінки з мобільного телефону та тексти SMS-повідомлень автоматично фіксуються й накопичуються на сервері оператора мобільного зв'язку та можуть бути отримані слідчим.

Крадіжка особистих персональних і комерційних авторизаційних даних користувачів, конфіденційної інформації, ключів захисту, використання апаратного ресурсу «комп'ютера-жертви» з подальшою можливістю проведення DDoS-атак[1] і виконання «брехливих» транзакцій здійснюється шляхом використання із злочинною метою шкідливих програмних продуктів.

Останніми роками спостерігається стрімке зростання правопорушень у системах дистанційного банківського обслуговування (ДБО). Шахрайська схема розкрадання грошових коштів жертви складається з трьох основних етапів: отримання конфіденційної інформації для здійснення неправомірного доступу в систему ДБО та проведення шахрайської операції від імені жертви злочину з використанням його авторизаційних даних і ключів електронних засобів захисту, отримання грошових коштів. Для викрадення персональних (авторизаційних) даних користувача системи ДБО (логіна, пароля й ключа підпису) правопорушники часто використовують спеціальне шкідливе програмне забезпечення. Найчастіше це – модифікації добре відомих троянських програм із додатковими функціями, що дозволяють після певних неправомірних дій повністю «самоліквідуватися» без можливості відновлення.

Затвердження Стратегії кібербезпеки України[2], яка дозволяє побудувати національну систему кібербезпеки, підтверджує пріоритетність протидії кіберзлочинності серед напрямів політики держави й зумовлює проведення подальших досліджень щодо сутності, класифікації та способів виявлення цифрових слідів.

СУЩНОСТЬ ЦИФРОВЫХ СЛЕДОВ В КРИМИНАЛИСТИКЕ

Авдеева Г. К.

Сообщение посвящено исследованию сущности цифровых следов в криминалистике, определению понятия этого термина. Рассмотрены характеристики цифровых следов неправомерного доступа к работе компьютерных систем и систем дистанционного банковского обслуживания. Предложены пути поиска информации о преступнике по его следам в цифровом информационном пространстве. Сформулировано авторское определение термина «цифровой след», представляющий собой материальный невидимый след, содержащий криминалистически значимую информацию (сведения, данные), зафиксированную в цифровой форме на

[1] DDoS-атака (атака на зразок «відмова в обслуговуванні», від англ. Distributed Denial of Service) – атака одночасно з великої кількості комп'ютерів на обчислювальну систему з метою створення таких умов, за яких легальні користувачі системи не можуть дістатися системних ресурсів (серверів) (див.: *Дремлюга Р. И.* Интернет-преступность: монографія. Владивосток: Изд-во Дальневост. ун-та, 2008. С. 23).

[2] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL: http://zakon4.rada.gov.ua/laws/show/96/2016.

материальном носителе, и который может быть обнаружен, зафиксирован и исследован с помощью цифровых устройств.

ESSENCE OF DIGITAL TRACKS IN CRIMINALISTICS

Avdieieva H. K.

The message is devoted to the study of digital traces essence in criminalistics, the definition of the concept of this term. Consideration is given to the characteristics of digital traces of unauthorized access to the operation of computer systems and remote banking systems. The author suggests the ways of searching for information about the criminal according to his tracks in the digital information space. The message gives the wording of the author's term "digital trace", which is a material invisible trace containing criminalistic meaningful information (knowledge, data) fixed in digital form on a physical medium and which can be detected, recorded and examined by using digital devices.