УДК 343.98

Г. К. Авдєєва,
С. В. Стороженко

ЕЛЕКТРОННІ СЛІДИ : ПОНЯТТЯ ТА ВИДИ

Статтю присвячено дослідженню сутності електронних слідів у криміналістиці, визначено поняття цього терміна. Розглянуто характеристики електронних слідів неправомірного доступу до роботи комп'ютерних систем та систем дистанційного банківського обслуговування. Запропоновано способи пошуку інформації щодо злочинця за його слідами в цифровому інформаційному просторі. Сформульовано авторське визначення терміна «цифровий електронний слід», який являє собою матеріальний невидимий слід, що може бути виявлений, зафіксований і досліджений за допомогою цифрових електронних пристроїв та який містить будь-яку криміналістично-значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальному носії.

Ключові слова: *електронний слід, цифровий електронний слід, комп'ютерні злочини, інфомаційні технології.*

Постановка проблеми. Новітні інформаційні технології викликали появу й подальший стрімкий розвиток нових форм злочинності, а саме – злочинів, що вчиняються за допомогою використання таких технологій, через що вони отримали назву кіберзлочинів [1]. Останнім часом збільшилася кількість кібератак на енергетичні та транспортні структури, банки, окремі державні та приватні установи. Зокрема, за шість місяців 2016 року в Україні здійснено більше 500 кібератак на сайти Держказначейства, Міністерства фінансів та інших державних структур [2]. Жертвами правопорушень стають і фізичні особи. Зокрема, сума неправомірно знятих коштів з електронних платіжних карток українців у 2016 році порівняно з 2015 роком збільшилася в чотири рази – до 339,13 мільйона гривень [3]. Така небезпека спонукає правоохоронні органи приділяти більше уваги боротьбі з таким видом суспільно небезпечних посягань та їх попередженню. На сайті Національної поліції України навіть розміщено рекомендації щодо фіксації електронних слідів, які в подальшому можуть бути використані як докази при розслідуванні інтернет-шахрайства [4]. Однак, на жаль, технічний рівень засобів і методів злочинної діяльності часто перевищує рівень засобів боротьби з нею. Тому проблеми дослідження електронних слідів у криміналістиці на сьогодні є актуальними.

Аналіз останніх досліджень і публікацій. Питанням дослідження проблем боротьби зі злочинами у сфері використання інформаційних технологій учені-криміналісти приділяють значну увагу останні два десятиліття, однак у зв'язку зі стрімким розвитком інформаційних

технологій і швидкими змінами поколінь комп'ютерної техніки та програмного забезпечення існує нагальна потреба щодо подальшого дослідження в цьому напрямі для уточнення окремих наукових положень, зокрема виокремлення специфічних слідів комп'ютерних злочинів та розроблення способів їх виявлення.

Науковці активно дискутують не лише щодо сутності слідів злочинів у сфері використання інформаційних технологій, а й щодо їх найменування. Запропоновано такі найменування слідів цієї категорії: комп'ютерні сліди, віртуальні сліди, електронно-цифрові, інформаційні, комп'ютерно-технічні, тощо [5].

Найбільш вдалим та таким, що адекватно віддзеркалює сутність слідів злочинів зазначеної категорії є найменування «електронні сліди», що запропонували російські та вітчизняні вчені [6].

Електронні пристрої (телефони, смартфони, комп'ютери, портативні пристрої геолокації (GPS,Glonass), цифрові фотоапарати, відеореєстратори, веб-камери, мережеві маршрутизатори, платіжні системи та інші цифрові пристрої все частіше використовуються злочинцями і, як наслідок, сліди неправомірних дій залишаються в інформаційному просторі. Однак існуюча в криміналістиці традиційна класифікація слідів учинення тих чи інших злочинів практично не охоплює ті її види, які виникли при появі нових видів правопорушень (у т.ч. – у сфері використання інформаційних технологій) та традиційних злочинів з використанням інформаційних технологій.

Формування цілей. Метою статті є дослідження сутності електронних слідів як нового виду слідів у криміналістиці та формулювання визначення терміна «цифровий електронний слід».

Виклад основного матеріалу. Електронні сліди є новим об'єктом криміналістичного дослідження, а електронна техніка надає цій інформації значення джерела доказів. При цьому комп'ютерна техніка, інформаційні технології та окремі програмні продукти можуть слугувати як засобом учинення злочинів, так і предметом злочинного посягання. Характер слідової картини кіберзлочинів залежить від способів їх учинення та характеристик електронних засобів, за допомогою яких здійснюються злочинні посягання. Оскільки за останні 5-10 років цифрова техніка повністю замінила аналогову, у поле зору правоохоронних органів нині потрапляють саме цифрові електронні сліди, а не аналогові.

Електронний 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 електронних 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 з 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 й вивчені лише за допомогою певних цифрових електронних пристроїв. За аналогією, об'єктивну форму існування слідів впливу високої температури на лезо ножа можливо вивчати лише за допомогою спеціальних металографічних мікроскопів.

Автори вважають, що визначення терміна «цифровий електронний слід» має бути таким: «Електронні цифрові сліди - це матеріальні невидимі сліди, що можуть бути виявлені, зафіксовані й вивчені за допомогою цифрових електронних пристроїв та які містять будь-яку криміналістично-значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях».

Специфічними властивостями комп'ютерної інформації (у т.ч. – електронних слідів) є такі:

– відсутність нерозривного зв'язку з матеріальним носієм;

– динамічність, можливість миттєвого перенесення в просторі (навіть з однієї частини земної кулі в іншу);

– можливість зміни й знищення інформації будь-якого обсягу за короткі проміжки часу (також за допомогою видаленого доступу);

– ідентичність оригіналу інформації, що має електронну форму, і всіх його копій (незалежно від виду носія інформації).

Основними об'єктами, які утворюють і сприймають електронні 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 банківських карт, мобільні телефони, планшети тощо. Крім того, що в них зафіксовано електронні цифрові сліди, пов'язані з подією злочину, окремі електронні модулі цих засобів дозволяють 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. Ці геолокації також можуть бути використані для встановлення факту одночасної присутності двох і більше осіб в одному місці, а неодноразове повторення таких фактів свідчить про їх взаємодію.

Важливу роль у формуванні слідової картини кіберзлочинів відіграють способи вчинення злочинів цієї категорії. Так, одним зі способів їх учинення є використання зі злочинною метою шкідливих програмних продуктів для крадіжки особистих персональних і комерційних авторизаційних даних користувачів, конфіденційної інформації, ключів захисту, використання апаратного ресурсу «комп'ютера-жертви» з подальшою можливістю проведення DDoS-атак [7], несанкціонованої розсилки повідомлень і виконання «брехливих» транзакцій. Такі неправомірні дії є найбільш поширеними правопорушеннями в банківській сфері України [8].

Електронні сліди також утворюються внаслідок зовнішнього доступу до комп'ютерних систем для 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, результати роботи антивірусних і тестових програм тощо. Вони можуть бути виявлені при експертному дослідженні комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду тощо.

Сліди неправомірного доступу до інформації можна виявити в мережі Інтернет, а згодом, виходячи з їх ознак - установити вихідне підключення й технічний засіб, з якого здійснювалося це правопорушення. Найменування й адресу інтернет-провайдера [9], за допомогою якого правопорушник підключений до мережі Інтернет, можна вільно отримати через спеціальну службу Whois (у мережі Інтернет), зазначивши IP-адресу «атакуючого» комп'ютера.

Час роботи користувача в мережі Інтернет можна встановити за спеціальним log-файлом (журналом). Додаткові відомості про вид, порядок і час підключень користувача до мережі і збіг цих даних з log-файлом провайдера може слугувати вагомим доказом несанкціонованого доступу до певної комп'ютерної системи.

Сліди неправомірного доступу до інформації містяться в журналах операційних систем та 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.

Важливу криміналістично-значущу інформацію можна отримати при вивченні даних електронного листування й сервісів обміну SMS-повідомленнями [10]. В атрибутах файлів електронних листів міститься дата й час відправлення, електронна адреса відправника, найменування та адреса інтернет-провайдера та інша інформація. Телефонні дзвінки з мобільного телефону й тексти SMS-повідомлень автоматично фіксуються й накопичуються на сервері оператора мобільного зв'язку. У багатьох випадках саме ці сліди дозволяють установити організаційні злочинні схеми.

На сайтах соціальних мереж (наприклад, Facebook, Twitter, LinkedIn, Instagram тощо) можна виявити електронні сліди у вигляді повідомлень і коментарів осіб, що перевіряються, їх персональних даних (наприклад, електронну адресу), фотознімків і відеозаписів, історію пошукових запитів тощо. Ці сліди містять інформацію про час відвідування сайту й деякі персональні дані користувача (наприклад, електронну адресу), за якими можна здійснити пошук його номера телефону, дати народження, місця роботи та проживання, визначити коло спілкування та інтереси.

Останні два-три роки спостерігається стрімке зростання правопорушень у системах дистанційного банківського обслуговування (ДБО). ДБО - це комплекс сервісів віддаленого доступу клієнтів до банківських послуг, в основному, за допомогою комп'ютерних або

телефонних мереж. При цьому клієнт видалено (без візиту в банк) передає необхідні розпорядження, використовуючи інформаційні технології.

Системи ДБО в Україні розподіляються на такі види: система «Клієнт-банк» (PC-banking, remote banking, direct banking, home banking); інтернет-банкинг; мобільний банкинг. Шахрайська схема розкрадання грошових коштів складається з трьох основних етапів: отримання конфіденційної інформації для здійснення неправомірного доступу в систему ДБО, проведення шахрайської операції від імені користувача з використанням його авторизаційних даних і ключів електронних засобів захисту, отримання грошових коштів. Для розкрадання персональних (авторизаційних) даних користувача системи ДБО (логіна, пароля й ключів підпису) правопорушники часто використовують спеціальне шкідливе програмне забезпечення. Найчастіше - це модифікації добре відомих троянських програм з додатковими функціями, що дозволяють після певних неправомірних дій повністю «самоліквідуватися» без можливості відновлення.

На сьогодні активно здійснюється побудова міжнародної системи боротьби з цими видами злочинів, об'єднуються потрібні кадри, розробляються методики розслідування злочинів цієї категорії, уточнюються процедури взаємодії з міжнародними структурами й правоохоронними органами різних країн (у т.ч. – за допомогою телекомунікаційних засобів і систем).

Висновки. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою інформаційних та телекомунікаційних технологій. Об'єктами кіберзлочинів є персональні дані, банківські рахунки, паролі та інша інформація не лише окремих фізичних і юридичних осіб, а й державних структур: енергетичних об'єктів, транспортних та банківських установ. Тому дослідження сутності поняття «електронний слід» та визначення терміна «цифровий електронний слід» є вкрай важливим для визначення їх ознак та шляхів пошуку.

Автори вважають, що визначення терміна «цифровий електронний слід» має бути таким: «Електронні цифрові сліди - це матеріальні невидимі сліди, що можуть бути виявлені, зафіксовані й вивчені за допомогою цифрових електронних пристроїв та які містять будь-яку криміналістично-значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях».

У 2016 році в Україні відбувся значний прогрес у сфері боротьби з кіберзлочинністю, а саме: затверджено Стратегію кібербезпеки України, яка дозволяє побудувати національну систему кібербезпеки [11]; створено Національний координаційний центр кібербезпеки; Верховна Рада України прийняла за основу проект Закону України «Про основні засади забезпечення кібербезпеки України». Це підтверджує пріоритетність протидії кіберзлочинності серед напрямів політики держави та обумовлює проведення й надалі досліджень щодо сутності, класифікації та способів виявлення електронних слідів.

Використані джерела:

1. Шило О. Г. Проблемні питання досудового розслідування злочинів, учинених із застосуванням комп'ютерних технологій та/або використанням мережі інтернет // Міжнародні стандарти з кібербезпеки та їх застосування в Україні (матеріали «круглого столу» м. Харків, 19 квіт. 2016 року) / за ред. А. П. Гетьмана, Б. М. Головкіна. – Х. : Право, 2016. - С. 10-13.

2. Кібератаки на Україну коштують мільйони доларів. [Текст] . – [Електронний ресурс]. – Режим доступу: http://detector.media/infospace/article/122774/2017-02-02-kiberataki-na-ukrainu-koshtuyut-milioni-dolariv-sbu/. – Заголовок з екрана.

3. Уражаюча сума, яку торік украли в українців кібершахраї: найпоширеніші злочинні схеми. [Текст] . – [Електронний ресурс]. – Режим доступу: http://www.expres.ua/news/2017/01/26/225031-vrazhayucha-suma-torik-vkraly-ukrayinciv-kibershahrayi-nayposhyrenishi. – Заголовок з екрана.

4. Ви стали жертвою інтернет-шахраїв? // Сайт Національної поліції України [Текст]. – [Електронний ресурс]. – Режим доступу: http://www.npu.gov.ua/uk/publish/article/896018. – Заголовок з екрана.

5. Див., наприклад: Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. ... канд. юрид. наук. М., 1997. - 215 с.; Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дис.... канд. юрид. наук. Воронеж, 2010. - 24 с.; Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... докт. юрид. наук. Воронеж, 2001. - 39 с.; Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. - №8. - С. 43-45 .; Сукманов В.О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений // Вестник Калининградского юридического института МВД России. С. 104–107.; Борисов В.В. Особенности фиксации информационных следов в практике защиты информации // Известия Южного федерального университета. Технические науки. Т.94. - 2009. - №5. - С. 164–168., с. 164–168; Шаповалова Г.М. Возможность использования информационных следов в криминалистике (вопросы теории и практики): дис. ... канд. юрид. наук. Владивосток, 2005. – 22 с.; Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: дис. ... канд. юрид. наук. М., 2007. – 22 с. та ін.

6. Див., наприклад: Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики Судебная экспертиза. Выпуск 2 (46) 2016 : научно-практический журнал. — Волгоград : ВА МВД России, 2016. — С. 10-19; Веліканов С. В. До поняття електронного сліду в криміналістиці // Досудове розслідування: актуальні проблеми та шляхи їх вирішення : матеріали постійно діючого наук.-практ. семінару, 27 лист. 2015 року / редкол.: С. Є. Кучерина (голов. ред.), В. В. Федосєєв (заст. голов. ред.) та ін. – Х. : Право, 2015. – Вип. № 7. – С. 241-244 та ін.

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

8. Транзакція - банківська операція, що полягає в переказі грошових коштів з одного рахунку на інший. – Див.: Финансовый словарь. [Текст] . – [Електронний ресурс]. – Режим доступу: http://finance.sci-lib.com/. – Заголовок з екрана.

9. Інтернет-провайдер (провайдер; від англ. internet service provider, скор. ISP — постачальник інтернет-послуги) — організація, що надає послуги доступу до мережі Інтернет та інші пов'язані з Інтернетом послуги.

10. SMS [англ. Short Messaging Service — «служба коротких повідомлень»] - технологія, яка здійснює приймання та передавання коротких текстових повідомлень за допомогою мобільного телефону. – Див.: Англо-русский словарь по вычислительной технике и программированию (The English-Russian Dictionary of Computer Science): около 55 тыс. статей. - 8-е изд., испр. и доп. © ABBYY, 2008; © Масловский Е.К., 2008. [Электронная версия]. – Заголовок з екрана.

11. Див.: Про рішення Ради національної безпеки й оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/96/2016. – Заголовок з екрана.

Стаття надійшла до редколегії 17.03.2017

Авдеева Г. К., Стороженко С. В. Электронные следы : понятие и виды

Статья посвящена исследованию сущности электронных следов в криминалистике, определению понятия данного термина. Рассмотрены характеристики электронных 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 электронный след», представляющий собой материальный невидимый след, который может быть обнаружен, зафиксирован и исследован с помощью цифровых электронных устройств и содержит любую криминалистически-значимую информацию (сведения, данные), зафиксированную в электронной цифровой форме на материальном носителе.

Ключевые слова: *электронный след, цифровой электронный след, компьютерные преступления, информационные технологии*.

Avdeeva G., Storozhenko S. E-traces : Concept and Types

The article is devoted to the study of the nature of crime traces in sphere of use of information technologies.

The definition of the term "e-trace " was proposed by some autors. In particular, the electronic digital traces are material invisible traces. They represent any important information for the crime investigation. This traces always are recorded in digital form on any physical information carrier.

The autors focused on the study of the set of traces of the most common ways of commission of computer crimes. The article has information about the electronic traces that appear as a result of using by criminals of e-mails and of text messeges. There are information about traces detection of unauthorized access to computers, to automated systems, to computer networks and to databases.

Computer crimes can be committed by means of telecom or computer networks and technolo-gies, with use of malicious software. Traces of computer crimes in form

of work of antivirus or test programs can be discovered during a forensic examination of computers and operation systems, of antivirus programs and application code, etc.

Traces of unauthorized access to information can be found in the Internet and then, according to their properties, a specific device can be established. The traces that indicate about an extraneous access to computer information are such: renaming of files and folders, changing of the size and/or files content, of their attributes, appearance of the new folders and files, time changing of the last access to data, their modification, etc.

The «Digital e-trace» is an unseen material trace that can be detected, recorded and studied by digital electronic devices and contained the forensically-relevant information (data) that recorded on a tangible digital data carrier.

The certain text messages (SMS) can be used as a evidences. They are stored on the servers of a mobile operator. Law enforcement authorities can access to information about the list of calls and text message. Important information can be gathered by studying the content of emails, instant messages and traces of unauthorized access to the remote banking systems. In many cases these traces allow to identify organizational schemes of crimes.

Currently the law enforcement authorities are executing formation of an international system for fighting with crimes of such kind actively. They are developing methods of investigation such crimes and are cooperating with international organizations and law enforcement agencies from different countries (including with the using of computer technologies). This determines the conduct of further research of nature of electronic traces, their classification and methods of detection.

Key words: *e-traces, digital e-traces, computer crimes, information technologies.*