УДК 343.98
DOI https://doi.org/10.32849/2663-5313/2019.6.58

Яна Найдьон,
юрисконсульт І категорії юридичного відділу
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

ПОШУК ТА ВИЛУЧЕННЯ ВІРТУАЛЬНИХ СЛІДІВ СТВОРЕННЯ ТА ПОШИРЕННЯ ІНФОРМАЦІЇ ПОРНОГРАФІЧНОГО ЗМІСТУ

У XXI столітті боротьба з комп'ютерною злочинністю є однією з першочергових проблем у світі. З кожним днем зростає кількість і якість кіберзлочинів, удосконалюються інформаційні й телекомунікаційні технології, відбувається постійна еволюція можливостей для вдосконалення комп'ютерних злочинів, отже, з'являються нові загрози для світових інформаційних мереж і всього суспільства загалом. Для розслідування й розкриття комп'ютерних злочинів неможливо застосувати традиційні технології, методики і способи виявлення слідів злочинів і формування доказів. У статті розглядаються проблемні питання пошуку та вилучення віртуальних слідів кіберзлочинів.

Ключові слова: віртуальні сліди, кіберзлочинність, кіберзлочин, криміналістика, пошук і вилучення віртуальних слідів.

Постановка проблеми. З виникненням і розвитком усесвітньої Мережі з'явився новий вид правопорушень – кіберзлочинність, яка з кожним роком набирає обертів і тягне за собою серйозні, а часом незворотні наслідки. Кількість кіберзлочинів в Україні з кожним роком зростає. Ще 2012 року американський спеціалізований журнал Computerworld присвятив велику статтю Україні, називаючи країну «раєм для хакерів», адже українські кіберзлочинці добре відомі у світі й несуть загрозу для багатьох країн. Сьогодні почалася реформа правоохоронних органів і створювана нині кіберполіція буде спецдепартаментом, який прийде на зміну нинішньому управлінню з боротьби з кіберзлочинністю. Для цього потрібно постійно вдосконалювати криміналістичну методику розслідування злочинів і надавати 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 в процесі розслідування злочинів, що вчиняються в мережі Інтернет [1, с. 51–52].

Досліджуваній у статті проблематиці, а також її окремим питанням присвячували праці такі науковці, як В.Ю. Агібалов, В.Д. Басай, Г.Л. Грановський, Є.П. Іщенко, А.В. Касаткін, В.А. Мещеряков, П.В. Мочагін, В.В. Поляков, О.А. Самойленко, О.Б. Смушкін, О.О. Сукманов, А.К. Шеметов та інші.

Метою статті є дослідження проблем пошуку та вилучення віртуальних слідів створення й поширення інформації порнографічного змісту як кіберзлочину.

Виклад основного матеріалу. Норма ч. 2 ст. 91 Кримінального процесуального кодексу України (далі – КПК України) визначає лише загальний алгоритм доказування, що полягає у збиранні, перевірці та оцінюванні доказів з метою встановлення обставин, що мають значення для кримінального провадження [2], залишаючи за рамками питання про види і специфіку доказової інформації, а також її подальше дослідження під час кримінального провадження, хоча така специфіка, очевидно, існує. Так, під час збирання доказів за злочинами проти громадського порядку та моральності, вчинених з використанням мережі Інтернет і мобільного зв'язку, виникає проблема, викликана тим, що частиною відомостей є комп'ютерна інформація, яка отримала в літературі назву віртуальної інформації. Характерною її рисою з погляду доказування є те, що вона може виступати як безпосередній слід злочину, так і носій такого сліду, тобто об'єкт-слідоносій. Як слід комп'ютерна інформація, як і будь-який слід, відображає факт взаємодії матеріальних об'єктів. Однак при цьому така інформація має відмінну якість: комп'ютерна інформація легко може бути змінена або знищена, причому вказані дії можуть проводитися дистанційно.

Традиційно в криміналістиці розрізняють матеріальні та ідеальні сліди: ті й інші опосередковують учинення злочинів проти громадського поряду та моральності загалом і створення й поширення інформації порнографічного змісту як кіберзлочину зокрема. Так, ідеальні сліди виникають, наприклад, у тому випадку, якщо потерпілий та обвинувачений спілкувалися через програму «Skype» із застосуванням відеотрансляції, де підозрюваний або обвинувачений демонстрував зображення і сцени порнографічного характеру тощо.

Автори, які вивчають питання розслідування злочинів у комп'ютерній сфері або з використанням комп'ютерної техніки, мережі Інтернет і мобільного зв'язку, пишуть про необхідність вилучення матеріальних слідів, а саме: слідів рук із поверхонь клавіатури, елементів системного блоку, модему [3, с. 53–55]. Однак варто зауважити, що доцільно такі сліди вилучати лише в тих випадках, коли злочинець користувався чужим електронним пристроєм. Однак найбільшу інформативність під час розслідування створення й поширення інформації порнографічного змісту як кіберзлочину мають так звані віртуальні сліди, які породжуються механізмом злочину, завершують дію цього механізму, іншими словами, об'єктивують зазначений механізм.

Неоднозначність природи віртуальних слідів викликає в криміналістиці широку полеміку, причому дискусія чималою мірою спрямована на вирішення питання, до матеріальних або ідеальних слідів належать віртуальні сліди. Разом із тим заслуговує на увагу підхід, відповідно до якого віртуальний слід розглядається як проміжна субстанція між матеріальними й ідеальними слідами. Відповідно, віртуальний слід розуміється як будь-яка зміна стану автоматизованої інформаційної системи, пов'язана з подією злочину й зафіксована у вигляді комп'ютерної інформації на магнітному носії, в т. ч. й на електромагнітному полі [4, с. 21]. Так, прикладом віртуальних слідів злочину може бути використання профілю в соціальних мережах (ВКонтакте, Instagram, Фейсбук, Однокласники, Твіттер тощо), де підозрюваний розповсюджував фото-, відеопродукцію порнографічного змісту як для загального доступу, так і в приватних повідомленнях.

Однак незалежно від поглядів на сутність віртуальної інформації як доказу в кримінальній справі вона повинна бути вилучена, зафіксована й оформлена відповідно до вимог чинного українського кримінального процесуального законодавства, яке стикається з низкою суттєвих труднощів і проблем, що нагально вимагають свого вирішення. Не претендуючи на повноту їх виявлення, доцільно звернути увагу на найбільш істотні та складні з них.

Збереження комп'ютерної інформації. Стосовно цієї проблеми в чинному українському кримінальному процесуальному й іншому галузевому законодавстві абсолютно не врегульоване питання про збереження комп'ютерних даних із моменту встановлення факту їх наявності до моменту вилучення (копіювання) в розпорядження досудового слідства, що є нагально необхідним для розслідування кіберзлочинів.

Така потреба може виникнути в тих випадках, коли слідством установлено, що будь-яка конкретна комп'ютерна інформація (відомості про повідомлення, що передаються по мережах електрозв'язку) надійшла, наприклад, на фізичний сервер конкретного провайдера, де знаходиться в масиві іншої інформації, накопиченої за конкретний період часу. Для її виділення із цього масиву й вилучення в інтересах слідства буде потрібен певний час, протягом якого інформація повинна залишатися незмінною. Забезпечення цього стане можливим, якщо органи, що здійснюють досудове розслідування, будуть наділені повноваженнями давати розпорядження про тимчасове збереження комп'ютерної інформації фізичним і юридичним особам, у розпорядженні яких вона знаходиться.

Багатьма країнами на законодавчому рівні це питання вже вирішено. Наприклад, законодавством США передбачена можливість направлення «запиту про збереження доказів злочину». Згідно з § 2703 (f) (1) Титулу 18 Зводу законів США, відповідно до такого запиту телекомунікаційні служби та Internet-провайдери зобов'язані за запитом урядових установ та органів ужити всіх необхідних заходів для збереження даних або інших відомостей, наявних у їхньому розпорядженні, до видання судом відповідного судового наказу, на основі якого ці дані вилучаються в розпорядження органів правосуддя. § 2703 (f) (2) Титулу 18 Зводу законів США встановлено, що компетентні органи мають право отримати запитувані дані протягом терміну їх зберігання, а саме протягом 180 днів [5, с. 897–898].

Фіксація слідів у вигляді комп'ютерної інформації. Закріплення й вилучення слідів комп'ютерних злочинів як у процесуальних режимах огляду, обшуку відповідно до чинного КПК України, так і в ході оперативно-розшукової діяльності фактично не забезпечує їх збереження в тому вигляді, в якому вони виявлені. Це зумовлено тим,

що «віртуальні сліди» в силу їх особливостей не можуть бути вилучені.

Може бути проведено лише їх копіювання з використанням різних програмно-технічних засобів, в ході якого обов'язково змінюються відображені в файлі дата й час останньої операції та замінюються датою й часом самого копіювання. Це тягне за собою втрату істотно важливої в доказуванні по таких справах інформації про фактичні дату й час створення копійованого файлу. Ця особливість ні в нормах чинного КПК України, ні в інших законодавчих актах не відображена, що істотно ускладнює визнання доказами скопійованої комп'ютерної інформації.

Копіювання комп'ютерної інформації, як правило, – це операція, що проводиться вручну шляхом послідовного управління цим процесом. Разом із тим обробка інформації в комп'ютерних мережах є швидкоплинним процесом, параметри якого, за винятком остаточних результатів, як правило, вручну фіксувати неможливо. За необхідності контролю й фіксації параметрів процесів переміщення інформації потрібне використання спеціальних програм, призначених для автоматичної реєстрації. Їх використання вимагає спеціальних знань, навичок і програм, робота з якими є компетенцією фахівця, а не слідчого.

Однак чинне кримінальне процесуальне законодавство, регламентуючи порядок залучення спеціалістів до участі в слідчих діях, не враховує зазначених особливостей слідів у сфері комп'ютерної інформації, а тому й не регламентує особливий (із застосуванням програмно-апаратних засобів) порядок їх фіксації (копіювання), не визначає особливих умов цього.

Відмова в цей час від розроблення кримінально-процесуальних приписів у цій сфері є серйозним недоліком, оскільки документування та копіювання відомостей про повідомлення, передані по мережах електрозв'язку, й інші «віртуальні сліди» нині досить ефективно застосовуються на практиці. Це відбувається в умовах, коли злочин, по-перше, відбувається на території країни, а по-друге, використані для його вчинення комп'ютерні мережі і їх складники (конкретні комп'ютери, сервери, провайдери) також знаходяться в межах території, на яку поширюється юрисдикція українських правоохоронних органів.

Відсутність правового регулювання, внаслідок чого суди не завжди визнають копію навіть відповідним чином документованої комп'ютерної інформації як доказ у кримінальних провадженнях, тягне за собою прийняття органами досудового слідства так званих заходів запобіжного характеру. Зокрема, в спірних випадках, коли копіювання інформації в силу властивого цій технічній дії режиму примусової зміни дати й часу останньої операції над файлами, сполученого з відсутністю можливості для його скасування, може перешкодити встановленню істини у провадженні, проводиться не копіювання інформації, а вилучення самих апаратних засобів комп'ютерної техніки. У подальшому вони надаються для експертних досліджень, висновки яких лише й визнаються доказами. Тим самим у кримінальному судочинстві штучно відбувається звуження кола доказів у провадженнях про злочини у сфері комп'ютерної інформації.

Прийняття подібних заходів запобіжного характеру також можливо лише у випадках, коли злочин, по-перше, відбувається на території країни, по-друге, використані для його вчинення комп'ютерні мережі і їх складники (конкретні комп'ютери, сервери, провайдери) також знаходяться в межах території, на яку поширюється юрисдикція українських правоохоронних органів.

Однак вилучення неможливо у випадках, коли злочини скоюються в глобальних комп'ютерних мережах, а «віртуальні сліди» знаходяться в сегментах таких мереж за кордоном країни.

Висновки

Отже, кіберзлочини залишають специфічну слідову картину: на місці події можна виявити як «традиційні» сліди, так і комп'ютерні сліди (віртуальні), що залишаються в пам'яті електронних пристроїв. Окреслені проблеми пошуку та вилучення віртуальних слідів кіберзлочинів, зокрема створення й поширення інформації порнографічного змісту, вимагають розроблення та внесення відповідних доповнень у кримінально-процесуальне законодавство України.

Список використаних джерел:

1. Романенко Т.В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет. *Молодий вчений.* 2016. № 1 (2).

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

3. Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации. *Сибирский юридический вестник.* 2004. № 1. С. 53–55.

4. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дисс. ... канд. юрид. наук. Воронеж, 2001.

5. Federal Criminal Code and Rules / Title 18 – Crime and Criminal Procedure (amendment received to February 15, 1999), West Group, St. Paul, Minn, 1999. P. 897–898.

В XXI веке борьба с компьютерной преступностью является одной из первоочередных проблем в мире. С каждым днем растет количество и качество киберпреступлений, совершенствуются информационные и телекоммуникационные технологии, происходит постоянная эволюция возможностей для совершенствования компьютерных преступлений, следовательно, появляются новые угрозы для мировых информационных сетей и всего общества в целом. Для расследования и раскрытия компьютерных преступлений невозможно применить традиционные технологии, методики и способы обнаружения следов преступлений и формирования доказательств. В статье рассматриваются проблемные вопросы поиска и извлечения виртуальных следов киберпреступлений.

Ключевые слова: виртуальные следы, киберпреступность, киберпреступления, криминалистика, поиск и извлечение виртуальных следов.

In the 20th century, fight against computer crime is one of the essential problems in the world. The number and quality of cybercrimes have been growing every day, information and telecommunication technologies have been improved and opportunities for computer crimes upgrading have been evolving. Therefore, new threats for world information networks and the whole society have appeared. It is impossible to implement traditional technologies, methods and ways of detecting tracks of crimes and forming evidence for investigating computer crimes. The article is aimed at looking into problems of search and eliminating of virtual cybercrime tracks.

Key words: virtual tracks, cybercrime, criminalistics, search and eliminating of virtual cybercrime tracks.