Бакал Анастасія Андріївна,
студент магістратури навчально-наукового інституту № 3 Національної академії внутрішніх справ

ПРОБЛЕМИ ПОШУКУ І ВИЛУЧЕННЯ ВІРТУАЛЬНИХ СЛІДІВ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ

Слідова картина комп'ютерних злочинів дуже специфічна і вимагає розробки принципово інших методів і засобів в порівнянні з традиційними. Сліди вчинення зазначених кримінальних правопорушень рідко залишаються у вигляді видимих змін навколишнього середовища. Вони в не розглядаються сучасною трасологією, оскільки в більшості випадків носять інформаційний характер, тобто є тими або іншими змінами в комп'ютерній інформації, що виражається у формі її блокування, копіювання, модифікації, знищення. Скоєння особою протиправних дій, пов'язаних з використанням комп'ютерних технологій спричиняє виникнення певної кількості слідів у тому числі і специфічних, притаманних лише зазначеній категорії. Саме тому використання цих інформаційних даних при розслідуванні є необхідною умовою забезпечення всебічного, повного й об'єктивного дослідження обставин кримінального правопорушення.

Характерна особливість віртуального простору полягає в тому, що взаємодіючі в ньому об'єкти, які беруть участь у процесі утворення слідів, не мають зовнішньої будови. Арсенал засобів і методів роботи зі слідами, накопичений трасологією, тут не працює, у зв'язку з чим ефективне розслідування в умовах інтенсивного розвитку комп'ютерних технологій потребує дослідження віртуальних слідів як нової категорії криміналістичної науки [1, с. 159].

Віртуальність, як елемент характеристики злочинів даного виду, пов'язується дослідниками з процесами обробки комп'ютерних даних:

– комп'ютерні системи забезпечують функціонування штучного середовища (віртуального середовища) у якому відбувається процеси обробки (циркуляція) комп'ютерних даних, а також можуть вчинятися протиправні впливи на ці процеси;

– механізм протиправного впливу на процеси обробки комп'ютерних даних (як і протидії його розслідуванню) має віртуальну складову, пов'язану з використанням процедур обробки комп'ютерних даних зі злочинною метою;

– протиправний вплив на процеси обробки комп'ютерних даних залишає нетрадиційні сліди (віртуальні сліди), які проявляються у: стані комп'ютерних даних, результатах їх обробки; режимах (характеристиках) процесів обробки комп'ютерних даних.

Віртуальні сліди розглядаються як будь-яка зміна стану автоматизованої інформаційної системи (утвореного нею «кібернетичного простору», пов'язана з подією кримінального правопорушення та зафіксована у вигляді комп'ютерної інформації (тобто інформації у вигляді, придатному для машинної обробки) на матеріальному носії, у тому числі й на електромагнітному полі. Зокрема вони характеризуються такими ознаками:

– існують на матеріальному носії, але недоступні для безпосереднього сприйняття;

– не мають фізично цілісної структури (віртуальний слід може складатися з великої кількості окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох фізичних носіях цифрової інформації);

– мають специфічний механізм слідоутворення;

– мають багатокомпонентний характер, складну інформаційну структуру, в якій поряд зі значущою кримінально-релевантною інформацією міститься значний обсяг допоміжних даних, що відповідають за цілісність і доступність комп'ютерної інформації віртуального сліду;

– вилучення віртуальних слідів можливе лише за допомогою спеціальних програмно технічних засобів;

– мають нестабільний характер, не мають міцного зв'язку із записуючим інформацію пристроєм, а також легко піддаються знищенню.

Останнім часом у сфері кіберзлочинності з'явилися нові тенденції. Однією з них є зміна тактики нападу. Сьогодні, розробники вірусів беруть до уваги те, що користувачі використовують новітні засоби захисту. На жаль, свідомими користувачами поки що можна назвати лише 50 % власників персональних комп'ютерів. Решта не вважає за необхідне застосовувати кіберпрофілактику.

Іншою тенденцією стало збільшення спаму на 250 %. Розробники вірусів вигадують новітні способи для того, щоб спонукати користувача перейти за посиланням на небезпечну адресу. Ще одна тенденція – використання шкідливих програм-додатків до різних файлів, що активуються під час завантаження на комп'ютер.

Найнебезпечнішим вірусом є CB-Locker. Це програма-здирник. Вона кодує всю інформацію на комп'ютері й пропонує його власнику оплатити певну суму за пароль для розблокування. Користувачеві дається кілька днів на роздуми, протягом яких сума зростає. По закінченні вказаного строку інформація знищується. При цьому вірус неможливо знешкодити. Єдиним способом захисту від нього, є створення резервної копії всіх файлів.

Ми вважаємо за потрібне запозичення Україною практики Казахстану, де більшість з тих, хто працює в Інтернеті, прирівнюються до представників засобів масової інформації, з подальшою можливістю притягнення до відповідальності за оперування неправдивими даними або такими, що посягають на честь та гідність особи. У нас притягнути

таких порушників до відповідальності практично неможливо. Проте навіть у судовій практиці є випадки, які спростовують це твердження. Так, гр. М. обвинувачували в неправдивій інформації, яку він розмістив на своїй сторінці у Фейсбуці. Той стверджував, що сторінка була зламана, а сам він не має до згаданої інформації жодного стосунку. З приводу цього навіть було відкрите кримінальне провадження, в рамках якого слідчий ініціював технічну експертизу. Її результати засвідчили, що ніякого зламу не було.

Ще один приклад. Гр. П. обвинувачували в тому, що з його IP-адреси була здійснена DoS-атака на сайт однієї з відомих партій. Постало питання ідентифікації. Державні експерти склали ключ, який нібито ілюстрував шлях атаки з IP-адреси гр. П. Водночас був залучений приватний експерт, який пояснив суду, що точну адресу атаки встановити неможливо, із чим, до речі, погодилися його колеги [2].

Тому виникає дуже багато запитань. Наприклад, як зафіксувати інформацію, яка є на екрані монітора? Засвідчення нотаріусом, для українських користувачів мережі сьогодні такої можливості немає. Тому виходом із ситуації може стати протокол, складений черговим райвідділу МВС про те, що за певною електронною адресою у певний час була розміщена певна інформація.

Правоохоронці зазначають, що складність доказування в царині кіберпростору полягає в тому, що це єдина сфера, де людина не може застосувати жодне з відчуттів. Досліджувати її можна лише опосередковано, і не завжди вдається зафіксувати те, що там відбувається.

При доказуванні фахівці радять виходити з таких умов:

– незмінність оригіналу. Будь-хто повинен мати змогу перевірити оригінал ще раз. Річ у тім, що коли цифровий пристрій використовується (навіть просто вмикається), в ньому фіксуються сліди, недоступні користувачеві. Тому, якщо комп'ютер став знаряддям вчинення кримінального правопорушення, його не можна вимикати (у такому разі інформація про підключення буде втрачена), так само як і перезавантажувати, оскільки можуть бути втрачені дані;

– повнота даних, необхідних для етапу розслідування. Наприклад, якщо не зберегти частину даних трафіку (обсяг інформації, що передається через комп'ютерну мережу за певний проміжок часу), не можна буде сказати, що до чого підключалось і що передавалось під час такого підключення;

– документування всіх етапів дослідження. Кожна особа, яка торкається комп'ютера, повинна залишити документ, в якому буде зазначено, що вона робила і з якою метою та кому робота була передана.

Таким чином, віртуальна реальність, стаючи частиною суспільного життя, закономірно стає і сферою здійснення кримінальних правопорушень, в межах якої виникають якісно нові типи слідів – віртуальні. Перспективами подальших досліджень у цьому напрямі є дослідження криміналістичних методів виявлення, фіксації, збереження та вилучення віртуальних слідів, способів аналізу та дослідження таких

слідів, а також подальше удосконалення окремих методологій розкриття кримінальних правопорушень у розрізі становлення віртуального сліду як самостійного елемента криміналістичної характеристики.

Список використаних джерел:

1. Хижняк Є. С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів. *Актуальні проблеми держави і права* : зб. наук. пр. / Видавничий дім «Гельветика», Одеса, 2017. Вип. 79. С. 159–166.

2. Узагальнення судової практики розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. URL : http://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446 FC2257B7C00499C02. Назва з екрана.

Безрученко Катерина Володимирівна,
курсант навчально-наукового інституту № 1
Національної академії внутрішніх справ

ПРОБЛЕМИ ДОПИТУ ЖІНОК – ПОТЕРПІЛИХ ВІД НАСИЛЬНИЦЬКИХ ЗЛОЧИНІВ

Ситуація з домашнім насильством в Україні достигла свого піку. Навіть Європейські партнери звернули на це увагу і вимагають від держави постійного захисту від домашнього насильства.

На законодавчому рівні дані заходи за останні два роки зрушилися із мертвої точки. Так, відповідно домашнє насильство закопилене в окремому Законі України «Про запобігання та протидію домашньому насильству». Відповідно до цього Закону під домашнім насильством розуміють – діяння (дії або бездіяльність) фізичного, сексуального, психологічного або економічного насильства, що вчиняються в сім'ї чи в межах місця проживання або між родичами, або між колишнім чи теперішнім подружжям, або між іншими особами, які спільно проживають (проживали) однією сім'єю, але не перебувають (не перебували) у родинних відносинах чи у шлюбі між собою, незалежно від того, чи проживає (проживала) особа, яка вчинила домашнє насильство, у тому самому місці, що й постраждала особа, а також погрози вчинення таких діянь [1].

Крім цього, у Кримінальному кодексі України також передбачена відповідальність за домашнє насильство. У законі про кримінальну відповідальність застосовано модель, яка передбачає окремий склад злочину – «Домашнє насильство» (ст. 126-1 КК України) та окрему кваліфікуючу ознаку певних складів злочинів (ч. 2 ст. 152, ч. 2 ст. 153 КК України) – «вчинення злочину щодо подружжя чи колишнього подружжя або іншої особи, з якою винний перебуває (перебував) у сімейних або близьких відносинах» [2].