Кривопуск Олександр Григорович
викладач кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ

ЩОДО ЗНАЧЕННЯ ВІРТУАЛЬНИХ (ІНФОРМАЦІЙНИХ) СЛІДІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛІСНОГО НЕВИКОНАННЯ ОБОВ'ЯЗКІВ ПО ДОГЛЯДУ ЗА ДИТИНОЮ АБО ОСОБОЮ, ЩОДО ЯКОЇ ВСТАНОВЛЕНА ОПІКА ЧИ ПІКЛУВАННЯ

Слідова картина будь-якого злочину є одним з ключових елементів криміналістичної характеристики. Кожне злочинне діяння характеризується змінами навколишнього середовища, що є результатом вчинення дій з підготовки, вчинення та приховування слідів злочинної діяльності.

У криміналістиці класично прийнятою вважається двокомпонентна структура слідової картини, яка охоплює матеріальні та ідеальні сліди. Проте останнім часом все частіше, крім ідеальних та матеріальних слідів, вчені криміналісти виділяють окрему групу слідів, під назвою віртуальні, або інформаційні, які залишаються внаслідок використання комп'ютерного обладнання або телекомунікаційних систем.

Переходячи до розгляду віртуальних слідів, які зберігають інформацію про вчинення злочину, передбаченого ст. 166 КК України, необхідно зауважити, що на сьогодні відсутній єдиний підхід щодо визначення поняття віртуальних (комп'ютерних) слідів. На думку Я. Найдьон, віртуальні сліди – це цифровий образ, електронні сигнали, що залишаються в пам'яті електронних і подібних до них пристроїв, що передаються за допомогою заданого алгоритму і мають кримінально-релевантне значення [1, с. 306].

В умовах стрімкого технологічного розвитку, який відбувається в нашій державі, відмічається тенденція зміни суспільних відносин, через що змінюється і злочинність, а це призводить до зростання кількості віртуальних (комп'ютерних) слідів, які залишають по собі злочинні діяння. Відносно нещодавно категорія віртуальних слідів розглядалась науковцями здебільшого в контексті вчинення окремих видів злочинів у сфері використання комп'ютерів та комп'ютерних мереж, виготовлення та розповсюдження порнографічної продукції, вчинення шахрайств за допомогою мережі «Інтернет» тощо. Проте на сьогодні практично кожне злочинне діяння може залишати інформаційні сліди, не є винятком вчинення злісного невиконання обов'язків по догляду за дитиною або особою, щодо якої встановлена опіка чи піклування.

З огляду на аналіз матеріалів кримінальних проваджень за ст. 166 КК

України, згідно з яким до основних джерел віртуальних (комп'ютерних) слідів можна віднести інформацію (фотознімки, відеозаписи із зображеннями потерпілого), що міститься на мобільних телефонах або смартфонах злочинця, потерпілого або свідків. Це твердження знаходить своє відображення у судових рішеннях, наприклад фрагмент Вироку Орджонікідзевського районного суду м. Запоріжжя від 10.06.2022: «… Коли приходив дільничний педіатр, їх не було вдома, і тому очно лікар дитину не оглядав. Вона (обвинувачена) спілкувалась телефоном із медичною сестрою, відправляла їй фотографії дитини…» [2].

Крім того, до типових віртуальних слідів, характерних також злісному невиконанню обов'язків по догляду за дитиною або особою, щодо якої встановлена опіка чи піклування, доречно віднести: сліди листування за допомогою електронної пошти в мережі «Інтернет» з лікарями або іншими третіми особами, які містяться в комп'ютерах, ноутбуках чи смартфонах злочинця, потерпілого або свідка; сліди листування за допомогою різних месенджерів, використовуючи при цьому комп'ютерну техніку та/або смартфони; сліди, які зберігаються на цифрових записах камер відеоспостереження громадських місць, місць масового відпочинку, де може міститись інформація про подію кримінального правопорушення, або дії потерпілого, підозрюваного чи інших учасників ні місці події. Істотного значення набуває інформація, яка міститься в розпорядженні операторів мобільного зв'язку, а саме інформація про розміщення пристроїв мобільного зв'язку на певних ділянках місцевості, що дозволяє висунути версії вчиненого кримінального правопорушення, встановити можливих свідків та осіб, які можуть бути причетними до вчинення злочину.

До окремої групи віртуальних слідів, характерних здебільшого злісному невиконанню обов'язків по догляду за дитиною або особою, щодо якої встановлена опіка чи піклування, пропонуємо відносити інформацію стосовно: подання заяв до органів влади або місцевого самоврядування, за допомогою електронних сервісів про реєстрацію новонародженої дитини (видачу свідоцтва про народження тощо), надання допомоги про народження дитини; електронних звернень до закладів МОЗ та отримання рецептів.

Підсумовуючи викладене, можна сказати, що з розвитком технологій все більшого значення для досудового розслідування набувають сліди відображені та які зберігаються на цифрових носіях інформації. Слідова інформація, що зберігається на комп'ютерних носіях, дозволяє більш глибоко зрозуміти механізм вчинення злочину цієї категорії, висунути версії щодо способу, обстановки та умов вчиненого злочину, особи злочинця, що допоможе ухвалити необхідні процесуальні рішення, ініціювати проведення слідчих (розшукових) дій, призначити необхідні судові експертизи та вибрати оптимальні шляхи досудового розслідування.

1. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304–307.

2. Вирок Орджонікідзевського районного суду м. Запоріжжя від 10 червня 2022 року URL: https://reyestr.court.gov.ua/Review/86407270 (дата звернення: 19.12.2022).

Лазарєв Владислав Олександрович
директор Навчально-наукового інституту
права та підготовки фахівців для
підрозділів Національної поліції,
кандидат юридичних наук,
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ ТА ЕКОНОМІЧНІ ЗЛОЧИНИ В МЕРЕЖІ DARK WEB В УМОВАХ ВОЄННОГО СТАНУ

Стрімкий розвиток інформаційних технологій в Україні та світі, який ми спостерігаємо останнє десятиріччя, невблаганно супроводжується динамічним розвитком злочинів у цій сфері. Масова комп'ютеризація та стрімкий розвиток цифрових технологій, які значно спростили життя людині, не стали винятком. Кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком кіберзлочини стають дедалі масовими й небезпечними.

Кіберзлочинність та економічні злочини в мережі Dark Web є серйозною загрозою для безпеки та фінансової стабільності.

Dark Web – це частина Інтернету, яка є прихованою та недоступною для пошуку за допомогою звичайних пошукових систем. Вона працює на основі технології невидимих мереж (наприклад, Tor), що приховують інформацію про сервери та користувачів. Це робить Dark Web ідеальним простором для злочинних дій.

Умовно Інтернет можна поділити на три прошарки. На поверхні – всім відомий Surface Web, або ж «поверхневий веб», який індексується стандартними пошуковими системами, такими як Google тощо [1].

«Глибинний інтернет» Deep Web, який містить у собі контент внутрішніх мереж корпорацій та університетів, або ж комерційні бази даних, до яких не може отримати доступ будь-хто та може бути у 400–500 разів більшим, ніж відомий нам Surface Web.

«Темний інтернет» Dark Web, контент якого прихований навмисно.