УДК 343.98
DOI https://doi.org/10.24144/2788-6018.2025.04.3.35

ОСОБЛИВОСТІ ТА ПРОБЛЕМИ ВИЯВЛЕННЯ Й ФІКСАЦІЇ ЦИФРОВИХ СЛІДІВ ПІД ЧАС ОГЛЯДУ МОБІЛЬНИХ ЗАСОБІВ ЗВ'ЯЗКУ

Курман О.В.,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики,
Національний юридичний університет імені Ярослава Мудрого
ORCID: 0000-0002-5432-7215

Курман О.В. Особливості та проблеми виявлення і фіксації цифрових слідів під час огляду мобільних засобів зв'язку.

Статтю присвячено особливостям та проблемам виявлення і фіксації цифрових слідів під час огляду мобільних засобів зв'язку. Сліди, що утворюються під час вчинення злочинів із використанням мобільних засобів зв'язку, – це інформація, зафіксована у цифровому форматі, яка міститься в різного роду цифрових пристроях, призначених для створення, оброблення, зберігання та передавання такої інформації, є причинно пов'язаною з подією кримінального правопорушення та дає змогу встановити як обставини вчиненого злочину, так і особу злочинця. Такі сліди в криміналістиці отримали назву цифрових.

Цифрові сліди можуть зберігатися як у операторів і провайдерів телекомунікацій, так і в самому мобільному телефоні (смартфоні). Будь-які дії злочинця, потерпілого чи інших осіб, які користуються послугами мобільного зв'язку, знаходять відображення на серверах оператора. Такий процес збирання, аналізу та систематизації інформації має назву білінг. Завдяки білінгу слідчий може отримати інформацію щодо: 1) номера SIM-картки абонента; 2) IMEI-номера мобільного пристрою; 3) дати, часу і тривалості виклику; 4) номера абонента, що здійснив виклик; 5) номера абонента, якого викликали; 6) імені абонента, якщо він верифікований; 7) вартості розмови; 8) номера базової станції на початку розмови; 9) номера базової станції наприкінці розмови.

У статті також розглянуто алгоритми рекомендованих дій слідчого під час безпосереднього огляду мобільного засобу зв'язку та запропоновано конкретні кроки щодо фіксації цифрових слідів, виявлених під час роботи з технічним засобом. Паралельно в роботі висвітлено деякі проблеми, пов'язані з використанням криміналістичних програмно-технічних комплексів. Зокрема, це пов'язано з тим, що засоби захисту смартфонів постійно вдосконалюються, відповідно – ускладнюється процес їх розблокування та вилучення даних. У разі випуску виробником нових версій протоколів безпеки операційних систем iOS і Android та їхнього оновлення на смартфоні виникають труднощі із реалізацією повного функціоналу програмно-апаратних комплексів мобільної криміналістики, а подекуди – й неможливість розшифрування даних.

Ключові слова: цифрові сліди, розслідування кримінальних правопорушень, слідчий огляд, методика розслідування, білінг, технічні засоби мобільної криміналістики, алгоритми дій слідчого, взаємодія зі спеціалістом.

Kurman O.V. Peculiarities and problems of detecting and recording digital traces during the inspection of mobile communication devices.

The article explores the peculiarities and challenges of detecting and recording digital traces during the inspection of mobile communication devices. Digital traces left in the course of crimes involving mobile communications consist of information recorded in digital format and stored on various devices used for the creation, processing, storage, and transmission of that information. These traces are causally linked to the criminal event and can help establish both the circumstances of the crime and the identity of the perpetrator. In forensic science, such evidence is referred to as digital traces.

These traces may be stored both on the servers of telecommunications operators and providers, as well as directly on the mobile device (e.g., smartphone). Any actions performed by the offender, victim, or other individuals using mobile communication services are typically recorded on the operator's servers. This process of collecting, analyzing, and organizing communication data is known as billing. Through billing records, an investigator can obtain the following information: 1) the SIM card number of the subscriber; 2) the IMEI number of the mobile device; 3) the date, time, and duration of each call; 4) the number of the calling subscriber; 5) the number of the called subscriber; 6) the name of the subscriber associated with the number (if verified); 7) the cost of the call; 8) the ID of the base station at the beginning of the call; 9) the ID of the base station at the end of the call.

The article also outlines recommended procedures for investigators conducting direct inspections of mobile communication devices and proposes specific steps for properly recording any digital traces discovered during such operations. At the same time, it highlights several challenges associated with the use of forensic software and hardware systems. A significant issue lies in the constant evolution of smartphone security features. When manufacturers release updated security protocols for iOS or Android and apply them to devices, it becomes increasingly difficult – if not impossible – for forensic tools to unlock the device or decrypt the data. This limits the effectiveness of current mobile forensic technologies.

Key words: digital traces, criminal offence investigation, investigative examination, investigative methodology, billing, technical tools of mobile forensics, investigator's action algorithms, cooperation with a specialistПостановка проблеми.

Постановка проблеми. Розвиток науково-технічного прогресу, використання штучного інтелекту, упровадження сучасних досягнень науки і техніки в практику вчинення кримінальних правопорушень зумовлює необхідність вдосконалення науково-методичного та техніко-криміналістичного забезпечення розслідування злочинів, одним із пріоритетних напрямів якого стає використання спеціальних знань і спеціальної криміналістичної техніки.

Стан опрацювання проблематики. Проблеми виявлення, фіксації та дослідження специфічних слідів в цифровому середовищі та використання спеціальних знань у ході досудового розслідування привертали увагу цілої плеяди вчених-криміналістів, зокрема: Демидової Є.Є. [1, с. 71–75], Коваленко А.В. [2, с. 202–214], Колеснікової І.А. [3, с. 472–475], Латиш К.В. [4, с. 165–172], Шевчука В.М. [5, с. 812–815], Шепітько В.Ю. [6] тощо. Однак, з урахуванням швидкозмінних процесів у технічному розвитку, зокрема в галузі телекомунікацій, зазначені проблемні питання потребують постійного наукового дослідження та доопрацювання.

Мета статті: дослідити особливості отримання, вилучення, вивчення інформації, що зберігається в мобільних телефонах або смартфонах, виявити проблемні моменти процедури дослідження.

Виклад основного матеріалу. Одним із найпоширеніших видів технічних засобів, що використовуються злочинцями під час вчинення правопорушень, є мобільні телефони (смартфони), за допомогою яких узгоджуються та координуються злочинні дії співучасників, висуваються погрози і здійснюється вимагання грошових коштів або майна, підшукують та вербують нових виконавців, визначають дії спільників із підготовки та приховування злочинної діяльності, збирають інформацію щодо майбутніх жертв, фіксують результати своїх дій для звітування, реалізують шахрайські схеми заволодіння чужим майном тощо. Сучасні можливості засобів мобільного зв'язку дають змогу здійснювати дзвінки та обмінюватися повідомленнями за допомогою стільникового зв'язку, проводити фото та відео зйомку, спілкуватися та передавати великі об'єми інформації через месенджери (Telegram, WhatsApp, Viber, Signal тощо), моніторити соціальні мережі та інтернет-простір.

Механізм слідоутворення під час використання засобів мобільного зв'язку має свою специфіку, оскільки утворені ними сліди, маючи інформаційний характер, не відображаються у зовнішній матеріальній обстановці. Використання спеціальних знань під час розслідування кримінальних правопорушень дає змогу не тільки виявити й зафіксувати залишені за допомогою мобільних засобів стільникового зв'язку сліди злочинної діяльності, але й встановити місцезнаходження злочинця або потерпілого, визначити маршрут їхнього переміщення, відновити текстову й мультимедійну інформацію, передану за допомогою мобільного пристрою, з'ясувати приналежність переданих даних конкретній особі.

Сліди, що утворюються під час вчинення злочинів із використанням мобільних засобів зв'язку – це інформація, яка зафіксована в цифрову форматі, міститься в різного роду цифрових пристроях зі створення, оброблення, збереження та передачі цієї інформації, причинно пов'язана з подією кримінального правопорушення, та дає змогу встановити як обставини вчиненого злочину, так і особу злочинця. Іншими словами такі сліди отримали назву цифрових, під якими розуміють дані, що залишаються в цифровому просторі внаслідок використання цифрових пристроїв, технологій та інформаційних мереж, які можуть бути використані в кримінальному провадженні й судочинстві [7, с. 396].

Інформація (цифрові сліди), яка зберігається у операторів та провайдерів телекомунікацій, відіграє важливу роль у процесі кримінального провадження. Встановлення особи, що користувалася послугами мобільного зв'язку, надає можливість органам досудового розслідування отримати відомості про ймовірного правопорушника, його соціальні зв'язки, а також характер і обставини протиправної діяльності. Будь-які дії злочинця, потерпілого чи інших осіб, які користуються послугами мобільного зв'язку, знаходять відображення на серверах оператора.

Такий процес збирання, аналіз та систематизації інформації отримав назву – білінг. В сучасних телекомунікаційних компаніях білінг – це складний комплекс програм, який дозволяє реалізувати процес збору інформації про використання телекомунікаційних послуг, тарифікацію, виставлення рахунків й обробку платежів споживачів послуг фіксованого і мобільного зв'язку, доступу до мережі Інтернет, інтернет-телефонії [8].

Будь-який оператор мобільного зв'язку здійснює постійне стеження за мобільними пристроями абонентів, використовуючи регістри положення і пересування, формуючи на сервері оператора базу даних білінгу: 1) номер SIM-картки абонента; 2) IMEI-номер мобільного пристрою; 3) дата, час і тривалість виклику; 4) номер абонента, що викликає; 5) номер абонента, який викликається; 6) ім'я абонента, відповідне до номеру, якщо він верифікований; 7) вартість розмови; 8) номер базової станції початку розмови; 9) номер базової станції закінчення розмови.

Встановлення місцезнаходження підозрюваного, потерпілого або будь-якої іншої особи може здійснюватися за допомогою можливостей технічних засобів операторів стільникового зв'язку або ж із використанням слідчими спеціалізованої криміналістичної техніки. Як правило, на етапі відкриття кримінального провадження підозрюваний невідомий і, запросивши дані білінгу, слідчий отримує масив даних про здійснені з'єднання абонентів за вказаний період часу в межах відповідної базової станції біля місця вчинення кримінального правопорушення. У подальшому, слідчий, аналізуючи отримані дані, виділяє збіги за датою, місцем і часом, після чого здійснюється перевірка конкретних SIM- та IMEI-номерів.

Зазначена інформація може бути отримана слідчим у порядку проведення тимчасового доступу до речей і документів, що є заходом забезпечення кримінального провадження. Ухвала надається оператору мережі мобільного зв'язку, у володінні якого знаходиться необхідна інформація, після чого відповідна службова особа зобов'язана надати тимчасовий доступ до зазначеної інформації з метою її вилучення або виготовлення необхідних копій. У подальшому отримана комплексна інформація (щодо абонентського номера оператора мобільного зв'язку) аналізується, а в разі необхідності отримання додаткової інформації, яка має значення для кримінального провадження, можливе проведення негласних слідчих (розшукових) дій, наприклад, зняття інформації з електронних комунікаційних мереж (ст. 263 КПК України) або ж установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ст. 268 КПК України) [9, с. 118]. У статтях 159, 162 КПК передбачено отримання слідчим (прокурором) інформації про зв'язок, що відбувся в минулому (постфактум), у тому числі про місцезнаходження радіоелектронного засобу у певний день та час. Особа, зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, зобов'язана згідно з ч. 1 ст. 165 КПК надати тимчасовий доступ до визначених в ухвалі речей або документів особі, вказаній у відповідній ухвалі слідчого судді, суду або ж особі, уповноваженій на здійснення тимчасового доступу на підставі доручення слідчого [10, с. 13].

На стадії вчинення та безпосереднього приховування слідів та наслідків вчинення злочину причетною особою можуть вчинятися дії, пов'язані зі знищенням або зашифровуванням інформації в самому мобільному пристрої (видалення листувань, фото та відео зображень, чистка історії браузера, блокування доступу до відповідної інформації в телефоні тощо).

Для якісного і своєчасного вилучення електронно-цифрових слідів застосовуються спеціальні апаратно-програмні комплекси мобільної криміналістики. Для отримання інформації з мобільних терміналів підрозділи Національної поліції України активно застосовують такі апаратно-програмні комплекси як «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC Physical Analyzer». Зокрема, такі комплекси використовують у своїй роботі оперативно-технічні підрозділи Національної поліції України та ДНДЕКЦ МВС України [11, с. 71] під час проведення: 1) відповідних оперативно-технічних заходів та негласних слідчих (розшукових) дій зі зняття інформації з електронних інформаційних систем; 2) слідчої (розшукової) дії як-то: огляд місцевості, приміщення, речей, документів та комп'ютерних даних (ст. 237 КПК України), для огляду мобільного терміналу (стільникового радіотелефону) та/або SIM-картки, виявлених на місці вчинення кримінального правопорушення; 3) обшуку житла чи іншого володіння особи, обшуку особи (ст. 236 КПК України) для доступу до комп'ютерних систем або їх частин, мобільних терміналів (стільникових радіотелефонів) та/або SIM-карток [12, с. 6].

Зазначені апаратно-програмні комплекси надають можливість пошуку і вилучення інформації, що зберігається в телефоні, комп'ютерному пристрої, а також у хмарному сховищі (iCloud, Google, Dropbox), навіть якщо пристрій є заблокованим. Програма дає змогу отримати дані з мобільних пристроїв та їхніх резервних копій, незалежно від особливостей операційних систем. У результаті програмне забезпечення створює повний образ досліджуваного пристрою, зокрема, дані зашифрованих застосунків, які виявляються і розшифровуються в максимальному обсязі та є повністю ідентичними даним застосунку на досліджуваному пристрої.

Істотною перевагою даного апаратно-програмного комплексу є можливість дослідження неробочого смартфону (наприклад, підданого тривалому знаходженню у воді або у разі, якщо неробочий стан виник внаслідок фізичного впливу, тощо). Крім смартфонів, що працюють на iOS і Android, програма підтримує менш популярні операційні системи, наприклад, Windows Phone, BlackBerry OS тощо. Пріоритетною функцією UFED є пошук і вилучення інформації з прихованих джерел (видалене листування в месенджерах, контакти, фотографії та відеозаписи). Дане програмне забезпечення надає можливість визначення за відновленими координатами GPS, що зберігаються в смартфоні під час користування, маршруту переміщення.

Розкриття та розслідування кримінальних правопорушень, що вчиняються з використанням мобільних засобів зв'язку, вимагає наявності спеціальних знань і навичок у дослідженні інформаційного простору вилученого пристрою. Якщо слідчий приймає рішення здійснити огляд самостійно, він повинен дотримуватися певних криміналістичних рекомендацій.

Слідчий огляд мобільного засобу зв'язку передбачає дві стадії – статичну та динамічну [13, с. 533]. Слідча дія розпочинається із загального огляду пристрою. У протоколі зазначаються: 1) модель телефону (смартфона), його форма, колір, розмір, назва, логотип; 2) наявність вбудованої фото- або відеокамери з тильної чи лицьової сторони; 3) розташування вбудованих функціональних і сенсорних клавіш; 4) наявність роз'ємів micro-USB або Type-C для підключення зарядного пристрою, стереонавушників, отворів для динаміків і мікрофона.

У разі наявності відповідної можливості та за умови необхідності, зумовленої конкретною слідчою ситуацією, слідчому рекомендується скористатися допомогою спеціаліста та техніко-криміналістичними засобами для розблокування телефону, якщо на ньому встановлено один із способів захисту: 1) буквено-цифровий пароль; 2) PIN-код; 3) графічний ключ; 4) ідентифікація за обличчям (фейс-контроль) тощо.

У протоколі огляду слідчий повинен зафіксувати процедуру розблокування телефону (смартфона) та подальші дії у хронологічному порядку. Після розблокування мобільного пристрою здійснюється опис графічних і текстових елементів, що відобразилися у центральному вікні екрана та в інших додаткових вікнах.

Криміналістично значущу інформацію можна виявити шляхом перегляду вмісту пристрою: журналу дзвінків, SMS-повідомлень, електронної та голосової пошти, історії використання веббраузера (вміст папок «Вибране», «Журнал», «Cookies», «Temporary Internet Files»), даних із месенджерів (WhatsApp, Viber, Telegram тощо), фото- та відеофайлів, диктофонних записів, органайзера – залежно від моделі телефону (смартфона).

Під час огляду вмісту мобільного засобу зв'язку спеціаліст, за вказівкою слідчого, проводить поетапну детальну фотозйомку екрана мобільного пристрою, фіксуючи інформацію, що має значення для розслідування. Для візуальної фіксації великого обсягу інформації, що зберігається в пам'яті технічного пристрою, рекомендується використовувати методи, способи та прийоми криміналістичного відеозапису. У такому разі слідчий обов'язково коментує всі дії та маніпуляції, які здійснюються для отримання тієї чи іншої інформації з телефону (смартфона).

У той же час необхідно зазначити, що існують певні технічні обмеження та проблеми з використанням таких криміналістичних програмно-технічних комплексів. Кінцева мета слідчого за допомогою криміналіста - отримати доступ до інформації, яка зберігається в захищених пристроях або в зашифрованому вигляді. Засоби захисту смартфонів постійно вдосконалюються; відповідно, ускладнюється і процес їхнього розблокування та вилучення даних. У разі випуску виробником останньої версії протоколів безпеки операційних систем iOS і Android та їхнього оновлення на смартфоні, виникають труднощі з реалізацією повного функціоналу зазначених програмно-апаратних комплексів мобільної криміналістики, а подекуди й неможливість розшифровування даних. Зазначена ситуація вимагає від розробників криміналістичних програмно-технічних комплексів постійного оновлення своїх знань щодо особливостей нових пристроїв, операційних систем і методів шифрування. Інструменти, які вони надають, не завжди сумісні з останніми моделями мобільних пристроїв або численними варіаціями регіональних або операторських версій смартфонів.

Висновки. На сьогодні існують різні механізми отримання слідчим важливої для розслідування інформації у вигляді цифрових слідів, які створюються під час використання мобільних засобів зв'язку. Такі сліди можуть бути виявлені в результаті проведення різноманітних процесуальних дій як безпосередньо слідчим, так і за участю спеціаліста із застосуванням сучасних програмно-апаратних комплексів мобільної криміналістики, якщо доступ до вмісту технічних засобів є обмеженим або ускладненим через певні обставини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету*. 2024, Серія Право. Вип. 85: част. 4. С. 71–75. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/12-3.pdf (дата звернення: 14.07.2025).
2. Коваленко А.В. Класифікація електронних (цифрових слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 202–214. URL: http://plaw.nlu.edu.ua/issue/view/16823 (дата звернення: 14.07.2025).
3. Колеснікова І.А. Цифрові сліди: поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал.* 2023. № 10, С. 472–475. URL: http://lsej.org.ua/10_2023/114.pdf (дата звернення: 14.07.2025).
4. Латиш К.В. Криміналістичний аналіз кіберінструментів вчинення злочинів. *Проблеми законності*. 2021. Вип. 153. С. 165–172. Режим доступу: http://nbuv.gov.ua/UJRN/Pz (дата звернення: 14.07.2025).
5. Шевчук В.М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. Військові правопорушення та воєнні злочини: історія, теорія та практика. Колективна монографія. "Izdevnieciba "Baltija Publishing" (м. Рига, Латвія), 2023. С. 795–822. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/ view/322/8791/18392-1 (дата звернення: 14.07.2025).
6. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія / В.Ю. Шепітько, Г.К. Авдєєва, В.М. Шевчук та ін.; за заг. ред. В.Ю. Шепітька. Харків: Право, 2024. 208 с.
7. Криміналістика: підручник / В.М. Шевчук, В.А. Журавель, В.Ю. Шепітько та ін.; за ред. В.М. Шевчука. Харків: Право, 2024. 1008 с.
8. Сертифікація білінгових систем в Україні. URL: http://oniis.org/ukr/poslugi/sertifikaciya-obladnannya-zvyazku/sertifikaciya-bilingovih-sistem-v-ukraini_(дата звернення: 14.07.2025).
9. Кузубова Т.О. Розвиток законодавчих положень, що регламентують тимчасовий доступ до речей і документів в України. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 2. С. 117–123. URL: https://dspace.univd.edu.ua/items/d6ab6f17-2a01-407a-a288-d51d5ee4488b (дата звернення: 14.07.2025).
10. Використання інформації, що знаходиться в операторів та провайдерів телекомунікацій у кримінальному провадженні: метод. рек. / [О.В. Таран, О.М. Брисковська, О.С. Тарасенко, А.А. Вознюк та ін.]. Київ: Нац. акад. внутр. справ, 2021. 50 с. URL: https://elar.naiau.kiev.ua/bitstreams/28ffc35c-c1e5-4583-8e16-2954c8bdd641/download (дата звернення: 14.07.2025).
11. Кобець М.В. Апаратно-програмний комплекс «Cellebrite UFED» як засіб отримання інформації з мобільних терміналів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану*: матер. міжвідоч. наук.-практ. конференції (м. Київ, 30 берез. 2023 р.). Київ: Нац. акад. внутр. справ. 2023. С. 70–73. URL: https://elar.navs.edu.ua/items/71ba959b-a48b-468d-a611-cad52e202482__(дата звернення: 14.07.2025).
12. Тіхонов С.В., Кобець М.В. Застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень: метод. рекомендації. Київ: Нац. акад. внутр. справ, 2023. 41 с. URL: https://elar.navs.edu.ua/items/eb658e56-3060-413b-9e01-6f797ce3e731_(дата звернення: 14.07.2025).
13. Курман О.В. Мобільні телекомунікаційні засоби як носії важливої доказової інформації: перспективність та проблеми дослідження. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 532–536. URL: https://app-journal.in.ua/wp-content/uploads/2023/10/APP_05_2023_FINAL.pdf (дата звернення: 14.07.2025).