Соціально-правові студії. 2020. Випуск 3 (9). С. 111-118
Social & Legal Studios. 2020. Issue 3 (9). P. 111-118

UDC (УДК) 343.102:343.132
JEL Classification: K 40

Климчук Михайло Павлович,
кандидат юридичних наук, доцент,
старший науковий співробітник науково-дослідної лабораторії
з проблем криміналістичного забезпечення та судової експертології
Навчально-наукового інституту № 2
Національної академії внутрішніх справ
(Київ, Україна)
e-mail: klymchuk1980@gmail.com
ORCID ID: 0000-0002-0488-5470

Кунтій Андрій Ігорович,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та криміналістики
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: kynt@ukr.net
ORCID ID: 0000-0001-5076-8358

ВИЯВЛЕННЯ ТА ВИЛУЧЕННЯ СЛІДІВ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, УЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ ЗАСОБІВ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Анотація. З'ясовано сутність слідів кримінальних правопорушень, учинених за допомогою засобів стільникового зв'язку. Уточнено окремі організаційно-тактичні та процесуальні аспекти виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням електронних носіїв інформації. Сформульовано пропозиції щодо удосконалення методики здійснення огляду мобільних пристроїв, зокрема, стосовно залучення до його проведення відповідного фахівця, використання необхідних спеціалізованих технічних засобів збирання слідової інформації тощо.

Ключові поняття: засоби стільникового зв'язку, електронні сліди, слідчі (розшукові) дії, огляд, виявлення доказів, вилучення доказів.

Klymchuk Mykhaylo,
PhD (Law), Associate Professor,
Senior Researcher, Research Laboratory of Forensic Science
and Forensic Expertise of the Institute № 2,
National Academy of Internal Affairs
(Kyiv, Ukraine)
e-mail: klymchuk1980@gmail.com
ORCID ID: 0000-0002-0488-5470

Kuntii Andrii,
PhD (Law), Associate Professor,
Associate Professor of the Department
of Criminal Proceedings and Criminology,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: kynt@ukr.net
ORCID ID: 0000-0001-5076-8358

DETECTION AND EXTRACTION OF TRACES OF CRIMINAL OFFENSES COMMITTED WITH THE USE OF CELLULAR COMMUNICATION MEANS

Abstract. It has been established that the development of information and telecommunications technologies has produced a large number of traces in various electronic devices, computer networks and elements of

their infrastructure, which must be used to establish the circumstances of the criminal act committed and the person involved. Emphasis has been placed on the fact that the circumstances causing the most significant problems in the detection and investigation of criminal offences committed by cellular means include, first of all, the complex mechanism of investigation, which requires the development of fundamentally different methods and means of their research. The methodological basis of the study is a set of general scientific and special methods and techniques of scientific knowledge, among them logic-semantic, statistical, abstraction, analysis, synthesis, analogy, abstraction and modelling. The nature and content of the traces of criminal offences committed by means of cellular communications have been clarified. The traces of a criminal offences committed by cellular means are classified into two types: traditional traces (physical traces in the form of traces-displays, traces of substances, traces-objects, also ideal traces, are considered by a trace) and non-traditional in the form of electronic (computer) footprints. Electronic copying of information is considered as a cognitive technique that can be used when inspecting a cellular communication means. The study of the possibilities of using electronic footprints, Big-data, technologies of working with them in criminal proceedings opens up new horizons for further development of forensics and its practical application in the light of realities. The specific organizational, tactical and procedural aspects of detecting and recovering traces of criminal offences committed using electronic media have been clarified; As a result, proposals have been formulated to improve the method of conducting inspections of mobile devices, in particular with regard to the involvement of a specialist; The use of the necessary specialized technical means for the collection of intelligence and the like.

Key concepts: means of cellular communication, electronic traces, investigative (search) actions, inspection, detection of evidence, seizure of evidence.

DOI 10.32518/2617-4162-2020-3-111-118

Вступ

Нині одним із технічних засобів, які найбільш часто використовуються у протиправних цілях, є засоби стільникового зв'язку. І це не випадково, адже, за даними компанії «Сіско», з 2013 до 2018 рр. світовий обсяг мобільного трафіка зріс майже в 11 раз і становить 15,9 ексабайтів. Окрім того, кількість підключених пристроїв до мережі Інтернет вже у 3,47 рази перевищує кількість населення світу, а у 2020 році прогнозується перевищення у 6,58 рази [1].

Засоби стільникового зв'язку часто є не тільки носіями криміналістично значущої інформації, а й предметами і знаряддями злочинів [2, с. 43]. Почастішали випадки «телефонного тероризму», коли злочинець за допомогою засобів зв'язку здійснює завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності. Поширені є й так звані «телефонні» шахрайства, коли телефоном повідомляють про необхідність надання фінансової допомоги родичам, які нібито потрапили в складну життєву ситуацію. Зазначені та інші кримінальні правопорушення, учинені за допомогою засобів стільникового зв'язку, завдають значної матеріальної шкоди, а через специфіку їх розслідування злочинцям вдається тривалий час залишатися безкарними [3, с. 85].

Певну проблему в розкритті та розслідуванні таких кримінальних правопорушень викликає така обставина, що механізм їх слідоутворення має свою специфіку, пов'язану з інтеграцією в мобільний телефон функціональних можливостей комп'ютера, і порівняно з традиційними слідами вимагає розробки принципово інших методів і засобів їх дослідження. Це пов'язано насамперед з тим, що такі сліди не залишають змін у зовнішньому матеріальному середовищі, адже в більшості випадків мають інформаційний характер. У зв'язку з цим вони зазвичай не вивчаються сучасною традиційною трасологією. Негативною обставиною для таких злочинів є легкість знищення слідів підготовки та вчинення протиправних дій. Водночас із використанням комп'ютерної техніки здійснюється вплив комп'ютерної інформації на комп'ютерну інформацію, яка може бути, з одного боку, носієм слідів, а з іншого – слідами вчинених злочинів.

Розвиток інформаційно-телекомунікаційних технологій обумовлює утворення великої кількості слідів у різних електронних пристроях, комп'ютерних мережах і елементах їх інфраструктури, які необхідно використовувати для встановлення обставин учиненого кримінального діяння і причетної до нього особи. Такі сліди пов'язані не тільки з кіберзлочинами, а й з іншими видами злочинних діянь.

Сучасні реалії обумовлюють формування тенденції до збільшення нових методів дослідження зазначених слідів та їх носіїв, що вимагає постійного підвищення кваліфікації слідчих, детективів, дізнавачів, інспекторів-криміналістів та експертів, удосконалення їхніх навичок, безперервного оновлення устаткування і програмного забезпечення, яке ними використовується. Відтак *мета статті* – уточнити окремі організаційно-тактичні та процесуальні аспекти виявлення та вилучення слідів

кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, сформулювати пропозиції щодо удосконалення методики здійснення огляду означених носіїв слідової інформації.

1. Методи та методики дослідження

Методологічну основу статті становить діалектичний підхід до процедури отримання, вилучення та зберігання інформації з мобільних засобів зв'язку у кримінальному провадженні. Для розв'язання завдань дослідження використано сукупність загальнонаукових і спеціальних методів і прийомів наукового пізнання. Застосований у роботі системний підхід надав змогу здійснити комплексне дослідження виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку. Логіко-семантичний метод допоміг ґрунтовно проаналізувати понятійний апарат. Методи абстрагування, аналізу, синтезу, аналогії, абстрагування та моделювання використано для розроблення пропозицій зі вдосконалення процедури вилучення, фіксації та зберігання слідової інформації, яка міститься у засобах стільникового зв'язку. Статистичний метод сприяв з'ясуванню сучасних тенденцій використання мобільного трафіка.

2. Сліди та їх класифікація

За використання засобів стільникового зв'язку у вчиненні кримінального правопорушення можна виявити матеріальні, ідеальні та електронні сліди, однак наразі серед учених немає одностайності у визначенні їх поняття та сутності.

Перший тип охоплює матеріальні сліди (сліди пальців рук, мікрочастинки), які можуть залишитися на корпусі мобільного телефону, SIM-картці та картці-пам'яті, акумуляторній батареї тощо, будь-які документи, рукописи, роздруківки тощо, які свідчать про приготування і вчинення кримінального правопорушення.

Ідеальні сліди, що відображають подію злочину й елементи механізму його вчинення у свідомості та пам'яті людей, мають психофізіологічну природу і виявляються у вигляді уявних образів злочину загалом, окремих його моментів і епізодів діяння [4, с. 56].

Електронні сліди – це інформація, зафіксована в цифровому форматі, що міститься в електронно-обчислювальних машинах та інших цифрових пристроях, створених на основі їхніх технологій, у засобах рухомого радіотелефонного зв'язку і на різних носіях цифрової інформації, причинно пов'язана з подією злочину, що дозволяє встановити обставини вчиненого і злочинця [5].

Пристроями, що містять електронні сліди злочину, які можуть використовуватися для встановлення обставин злочину та розшуку особи, яка його вчинила, зазвичай, є: мобільні телефони без підтримки сучасних додатків і смартфони, які підтримують такі додатки; стаціонарні комп'ютери, ноутбуки, нетбуки, планшети та інші малогабаритні комп'ютери; різні електронні гаджети (як-от, багатофункціональні електронні годинники, пульсоміри, крокоміри тощо); елементи інфраструктури інформаційно-комунікаційних мереж і операторів, що надають послуги зв'язку (сервери тощо); автомобільні відеореєстратори; GPS-навігатори та ін.

Найбільш інформативними є відомості, отримані з мобільних телефонів і смартфонів, що належать потерпілому і злочинцеві: про осіб з кола їх спілкування і зміст листування з ними (в адресній книзі, електронній пошті, соціальних мережах, месенджерах, текстових документах тощо); придбані електронні квитки на різні види транспорту, факти використання сервісів пошуку попутників для поїздок (приміром, BlaBlaCar); фінансові транзакції, здійснені за допомогою банківських та електронних платіжних систем, пов'язаних, наприклад, із придбанням туристичних путівок (з метою сховатися від органів слідства), бронюванням готелів, наймом житла (для тимчасового перебування там), орендою автотранспорту (для пересування); файли фотографій, що містять відомості про місце і час здійснення зйомки; інші використані такими особами електронні пристрої, пов'язані і синхронізуються з досліджуваним комп'ютером тощо, які можливо безпосередньо використовувати для встановлення обставин розслідуваної події і місця знаходження злочинця, що переховується; транспортні засоби, обладнані автосигналізацією з функцією супутникового охоронно-моніторингового сервісу та синхронізовані з досліджуваним комп'ютерним пристроєм. Така ж інформація може бути отримана зі смартфонів, які підтримують додатки, що дозволяють здійснювати комунікацію в мережі Інтернет і зберігати потрібну інформацію.

На нашу думку, сліди кримінального правопорушення, учинені за допомогою засобів стільникового зв'язку, варто розділити на два типи. До першого потрібно віднести традиційні сліди (матеріальні сліди у вигляді слідів-відображень, слідівречовин, слідів-предметів, також ідеальні сліди, що розглядаються трасологією) і нетрадиційні у вигляді електронних (комп'ютерно-технічних) слідів.

Механізм слідоутворення таких кримінальних правопорушень безпосередньо пов'язаний

із системою організації стільникового зв'язку. Тому певний інтерес становлять такі її основні елементи:

– апаратно-технічні засоби підтримки системи стільникового зв'язку, до яких можна віднести як базові, так і абонентські рухливі станції, центри комутації, ефірний інтерфейс;

– засоби інформаційної підтримки системи стільникового зв'язку, які містять програмне забезпечення, дані і бази даних, що дозволяють здійснювати свої функціональні можливості системи стільникового зв'язку;

– засоби допоміжної підтримки системи стільникового зв'язку. Це зазвичай центри технічного обслуговування, роботи з клієнтами тощо.

З огляду на розглянуту систему стільникового зв'язку, типовими для кримінальних правопорушень, учинених із використанням указаних засобів, будуть інформаційні сліди на машинних носіях оператора зв'язку. Скажімо, дані первинного номера телефону, який використовується для зв'язку з LOG-файлом реєстрації; дати сеансу зв'язку; інформація про час зв'язку; статичні або динамічні IP-адресні журнали реєстрації провайдера в Інтернеті і відповідні телефонні номери; швидкість передачі повідомлення; вихідних журналів сеансів зв'язку, що містять тип використаних протоколів, протоколи та ін. [6, с. 157]. Ними можуть бути й сліди на самому мобільному телефоні. Скажімо, IMEI-код, SMS-повідомлення, відомості про надіслані повідомлення, телефонні з'єднання, абонентська книга телефону, використовувані телефонні номери, сліди мікрочастинок, пальців рук. Сліди, присутні на SIM-карті і наявні на мобільному телефоні, зазвичай ідентичні.

На нашу думку, посиланню зацікавлених осіб на велику вартість технічних засобів, які підлягають використанню для цього, не повинно надаватися першочергове значення. Адже економічний ефект від припинення і розкриття злочинної діяльності у сфері комп'ютерної інформації буде набагато вищим від витрат, пов'язаних зі зберіганням відомостей про повідомлення, що передаються технічними каналами зв'язку. За статистикою, сьогодні збитки, завдані комп'ютерними злочинами, можна порівняти з прибутками від незаконного обігу наркотиків і зброї. Тільки в США щорічна економічна шкода від таких злочинів становлять близько 100 млрд дол. Однак багато втрат не виявляються або про них не повідомляють [7, с. 49].

3. Вилучення електронних носіїв інформації

Певні процесуальні та організаційно-технічні труднощі у кримінальному провадженні викликає процедура вилучення електронних носіїв інформації (комп'ютерних блоків, серверів, ноутбуків, карт пам'яті), їх повернення у разі вилучення та (або) копіювання інформації, яка міститься на них.

Спершу дослідимо процесуальні аспекти окресленої проблеми.

У ст. 258 КПК України визначено, що слідчий, прокурор зобов'язані звернутися до слідчого судді відповідного апеляційного суду (ст.ст. 246, 248, 249 КПК) з клопотанням про дозвіл, якщо будь-яка слідча (розшукова) дія охоплюватиме таке втручання [8]. Водночас досі поширеною є практика огляду уповноваженими суб'єктами кримінального провадження засобів стільникового зв'язку із втручанням в приватну переписку осіб без отримання відповідного дозволу. Згодом така інформація, відображена у протоколі огляду, використовується як доказ у кримінальному провадженні.

Такі порушення, допущені під час складання протоколу, є безумовною підставою для його визнання судом недопустимим доказом. Так, відповідно до п. 1 ч. 2 ст. 87 КПК України, суд зобов'язаний визнати істотними порушеннями прав і основоположних свобод учинення процесуальних дій, які потребують попереднього дозволу, але проведені без такого дозволу або з порушенням його суттєвих умов [8].

Зауважимо, що Верховний Суд у постанові від 9 квітня 2020 року у справі № 727/6578/17 зазначив, що якщо інформація, яка була наявна в мобільному телефоні, була досліджена органом досудового розслідування шляхом увімкнення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем, то це може бути оформлено як огляд предмета – телефону [9].

У ч. 2 ст. 264 КПК України вказано, що не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту [8]. Тому у разі, коли особа добровільно розблокує засіб стільникового зв'язку, слідчий має підстави безперешкодно здійснити огляд його вмісту, а отриману інформацію використати як доказ у кримінальному провадженні. Інакше судом ознайомлення з інформацією з електронного пристрою суд визнає втручанням у приватне спілкування, а протоколи огляду недопустимими доказами (див., наприклад, Вирок Селидівського міського суду Донецької області від 02 березня 2016 р.) [10].

Отримання та фіксування інформації, яка міститься на електронних пристроях (персо-

нальних комп'ютерах, ноутбуках, смартфонах, телефонах тощо), має здійснюватися на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів (у цьому випадку – документів у електронній формі) [11, с. 172]. Показово, що такий висновок підтверджується й судовою практикою (див., приміром, Ухвалу слідчого судді Солом'янського районного суду м. Києва від 20 вересня 2017 р.) [12].

У контексті досліджуваного питання слід зазначити, що, на нашу думку, змінами до абз. 2 ч. 2 ст. 159 КПК України законопроекту № 2740 від 15.01.2020 р. про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) цілком слушно запропоновано вдосконалити процедуру тимчасового доступу до речей і документів. Зокрема, тимчасовий доступ до пристроїв для обробки, передавання та зберігання електронної інформації або їх складових здійснюється без їх вилучення (виїмки) шляхом зняття копії інформації, що в них міститься. Результати копіювання інформації фіксуються у відповідному протоколі, що має містити опис усієї знятої інформації. Копія цього протоколу вручається особі, якій належить пристрій, з якого здійснено копіювання інформації, чи його представнику [13].

З огляду на мету статті, зосередимо увагу на тактичних та організаційно-технічних особливостях огляду засобу стільникового зв'язку.

Найпоширенішим способом процесуального оформлення дії, яка полягає в огляді та фіксації електронної інформації, що міститься на вилучених у межах інших процесуальних дій електронних пристроях, є складання слідчим протоколу огляду в порядку ст. 237 КПК України. На нашу думку, складність проведення такого огляду часто зумовлена відсутністю знань, необхідних для опису відповідного апаратного і програмного забезпечення (на базі операційних систем Android, iOS і WindowsPhone), недостатністю навичок із вилучення та збереження криміналістично значущої інформації з використанням апаратно-програмних комплексів (UFED, АДІС «Дакто 2000», Компоратор «Регула» 4305 DMH та ін.).

За проведення слідчої (розшукової) дії варто враховувати, що файли можуть перебувати як у пам'яті телефону, так і на картах пам'яті. У протоколі огляду слід зазначити їх виробника, обсяг і серійний номер карти, за наявності перемикачів захисту від запису (замка) – його положення. Після цього потрібно увімкнути захист від запису, щоби вимкнути модифікацію даних, які зберігаються на карті. Контакти, СМС-повідомлення і файли в пам'яті телефону повинні бути збережені на зовнішніх носіях за допомогою відповідного апаратного і програмного забезпечення. З цією метою може бути використаний програмно-апаратний комплекс UFED (Universal forensic extraction device), перевагою якого є більш широкі можливості використання, які дають змогу здійснювати повне вилучення таких даних, як телефонна книга, текстові повідомлення, фотографії, відео, журнали дзвінків (вихідні, вхідні, пропущені), звукові файли, ідентифікаційні дані телефону тощо.

З метою збереження інформації, яка міститься у засобі стільникового зв'язку, слід від'єднати його від Інтернет-мережі. Крім того, не рекомендується витягати карти пам'яті, сім-карти та інше апаратне забезпечення, яке знаходиться в телефоні.

Для уникнення знищення, пошкодження та зміни електронних слідів, що містяться на електронних носіях інформації, слідчому необхідно використовувати допомогу відповідного фахівця, який має необхідні знання, навички та обладнання. Фахівець у галузі комп'ютерних технологій може сприяти слідчому у виявленні в програмах для спілкування через Інтернет (Viber, WhatsApp, Telegram та ін.) криміналістично значущої інформації: про контакти; про зміст переписки між суб'єктами злочинної діяльності; про відеофайли; про дані розташування і маршрут руху, згідно з GPS; про найменування мереж Wi-Fi, до яких телефон раніше підключався.

Отже, електронне копіювання інформації слід розглядати як пізнавальний прийом, який може бути використаний під час огляду засобу стільникового зв'язку.

Під час вилучення засобу стільникового зв'язку слід звертати увагу на його стан. Якщо телефон увімкнений, то найкращим способом його ізоляції буде активування в ньому «автономного режиму» або режиму «в літаку». Вимкнення телефону може активувати засоби захисту (наприклад, ПІН-код для сім-карти і / або коди безпеки), які потім будуть потрібні для отримання доступу до пристрою, що може зашкодити проведенню експертизи. У разі наявності активованих засобів захисту (як-от «графічний ключ») варто відразу ж поцікавитися у власника телефону алгоритмом розблокування. Слід звертати увагу на дату і час, зазначені на екрані телефону, якщо він увімкнений, і порівнювати їх із поточним часом і датою на момент огляду, фіксуючи невідповідності.

Процедура вилучення доказів із засобів стільникового зв'язку відрізняється від вилучення інформації з персональних комп'ютерів з

огляду на те, що мобільні електронні пристрої, порівняно з персональними комп'ютерами, мають більш вузькі завдання, різну архітектуру процесора, операційну систему тощо. У зв'язку з цим методи і особливості проведення процесуальних дій повинні бути індивідуальними, залежно від технічних характеристик джерела доказів [14, p. 69].

Британською асоціацією керівників поліцейських служб була розроблена інструкція з вилучення доказів із мобільних пристроїв [15]. Згідно із запропонованими рекомендаціями, у проведенні процесуальних дій необхідно ізолювати пристрій від мобільного з'єднання шляхом вимкнення пристрою або завдяки спеціальним програмам, які глушать зв'язок пристроїв, усі необхідні процедури повинні проводитися в спеціально обладнаному приміщенні. Пристрій повинен бути повністю зарядженим з метою запобігання втрати інформації при проведенні процесуальних дій. Потрібно враховувати особливість оперативної (RAM) пам'яті пристрою, для збереження даних на якій необхідна наявність безперебійного живлення на відміну від постійної (ROM) пам'яті. З метою збереження важливої інформації спеціаліст повинен суворо дотримуватися правил, не допускати оновлення програм, позаяк це може спричинити знищення даних. Разом із даними додатків, які знаходяться на мобільному пристрої, необхідно також запросити відомості, що зберігаються на серверах розробників додатків, і дані інтернет-провайдера.

Сучасні смартфони, особливо iPhone, часто синхронізують із комп'ютером або ноутбуком. Відповідно, доцільним буде вилучення у власника смартфона комп'ютера або ноутбука (у разі надання ним такого дозволу). У випадку незгоди власника єдиною правовою підставою для вилучення електронного носія інформації може бути його вилучення у порядку ч. 3 ст. 233 КПК України у разі безпосереднього переслідування осіб, які підозрюються у вчиненні злочину. У такому випадку прокурор, слідчий за погодженням із прокурором зобов'язаний невідкладно після здійснення таких дій звернутися з клопотанням про проведення обшуку до слідчого судді. Слідчий суддя розглядає таке клопотання згідно з вимогами статті 234 КПК, перевіряючи, крім іншого, чи дійсно були наявні підстави для проникнення до житла чи іншого володіння особи без ухвали слідчого судді [8].

Наголосимо, що вилучення всіх засобів комп'ютерної техніки пришвидшує процес розслідування, дає можливість спрямувати основні зусилля на пошук інших матеріальних слідів, які стосуються злочину (документи, технічні засоби тощо), дає змогу в подальшому більш детально, залучаючи необхідних фахівців, вивчити інформацію, що міститься в пам'яті електронного носія інформації. Це практично виключає можливість пропустити навіть професійно приховану інформацію. Доцільність вжиття таких дій визначається слідчим у кожному окремому випадку залежно від слідчої ситуації у кримінальному провадженні.

Упаковка вилученого комп'ютерного засобу або накопичувача інформації повинна забезпечувати насамперед інформаційну цілісність, тобто унеможливити підключення кабелів електроживлення або периферійних пристроїв. Найкращим варіантом упаковки є поміщення вилученого стільникового засобу зв'язку в полімерний пакет. Під час його опису слід вказувати інформацію в тому обсязі, який дозволить однозначно ідентифікувати вилучений засіб. У більшості випадків достатньо вказати марку, модель, індивідуальний заводський номер пристрою. У разі, якщо з певних причин така інформація недоступна, слід указувати інші індивідуальні ознаки: розмір, колір, форму тощо. Бажано здійснювати фіксацію не тільки процесуальним способом, відображаючи вилучення електронного пристрою у протоколі слідчої (розшукової) дії, але й криміналістичним, фотографуючи його [16, с. 84].

Є низка спеціалізованих інструментів веб-аналітики, що дозволяють отримувати корисні для використання в розслідуванні аналітичні дані з відкритих джерел мережі Інтернет. Такі програми (деякі з них безкоштовні) спрямовані на отримання певної інформації у великому масиві данних, зокрема корисної для розслідування: про конкретну особу і її соціально-психологічний портрет: коло спілкування, психологічні особливості, зокрема емоційні, комунікативні, мотиваційні та ціннісно-моральні якості, а також дані про її психологічне благополуччя (наприклад, за профілями в соціальних мережах); про кілька сторінок однієї і тієї ж особи в різних соціальних мережах, і зареєстрованих під вигаданими даними, для його ідентифікації як їх єдиного користувача; про IP-ідентифікатор пристрою, який використовувався для виходу в мережу Інтернет в конкретних випадках (скажімо, для поширення екстремістських матеріалів, дитячої порнографії тощо); про деякі дії особи у разі її активності в мережі Інтернет (наприклад, за використаним ним номером телефону – для реєстрації в соціальних мережах і електронних платіжних системах, у розміщенні оголошень тощо).

Висновки

Отож до обставин, які зумовлюють найбільш істотні проблеми в розкритті і розслідуванні кримінальних правопорушень, учинених за допомогою засобів стільникового зв'язку, слід віднести насамперед складний механізм слідоутворення, який вимагає розробки принципово інших методів і засобів їх дослідження. Слідова картина таких кримінальних правопорушень безпосередньо пов'язана з системою організації стільникового зв'язку, що, своєю чергою, визначає сукупність необхідних для дослідження нетрадиційних електронних слідів. Зміст і межі використання спеціальних знань обумовлені специфікою розслідування і можуть бути значно ширшими на основі дослідження питань, що стосуються розвитку сучасних засобів комунікації, комп'ютерних технологій і телекомунікаційних мереж.

Вивчення можливостей використання електронних слідів, зокрема. Big data-даних, технологій роботи з ними у кримінальному провадженні, відкриває нові горизонти для подальшого розвитку криміналістики і її практичного застосування з урахуванням реалій сьогодення. Водночас за проведення огляду засобу стільникового зв'язку необхідно враховувати вимоги чинного КПК України та технічні особливості вказаної слідчої (розшукової) дії (залучення відповідного фахівця, використання необхідних спеціалізованих технічних засобів збирання слідової інформації).

Список використаних джерел

1. Интернет-трафик (мировой рынок). URL: https://www.tadviser.ru/index.php
2. Casey E., Turnbull B. Digital Evidence on Mobile Devices. Digital Evidence and Computer Crime. Third Edition. ACADEMIC PRESS, 2011. 44 p.
3. Климчук М. П. Сліди кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку, й особливості їх виявлення. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід*: матер. Міжнар. наук.-практ. круглого столу (м. Київ, 19 лют. 2020 р.). редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2020. С. 84–88.
4. Криминалистика : учебник; отв. ред. Н. П. Яблоков. 3-е изд., перераб. и доп. Москва : Юристъ, 2005. 781 с.
5. Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами. DOI: 10.17803/2311-5998.2019.55.3.046-052.
6. Потапов С. А., Потапова И. С. Использование экспертиз при расследовании и раскрытии преступлений, совершенных с применением сотовых телефонов. *Социально-экономические процессы и явления*. 2016. № 11. Т. 11. С. 155–161. DOI: 10.20310/1819-8813-2016-11-11-155-161.
7. Капинус О. С. Криминология. Особенная часть: в 2 т : монография. Москва : Издат. Юрайт. 2016. Т. 2. 311 с.
8. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua (дата звернення: 23.07.2020).
9. Постанова Верховного суду України від 09.04.2020. Справа № 727/6578/17; № 51-4494км19. URL: https://verdictum.ligazakon.net/document/ 88749345?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress05 (дата звернення: 23.07.2020).
10. Вирок Селидівського міського суду Донецької області від 02.03.2016. URL: http://www.reyestr.court.gov.ua/Review/56200716 (дата звернення: 23.07.2020).
11. Шило А. В. Отримання інформації з вилученої електронної техніки як спосіб збирання доказів: спірні питання практичного правозастосування. *Науковий юридичний журнал.* № 5/2018. С. 172–179.
12. Ухвала слідчого судді Солом'янського районного суду м. Києва від 20.09.2017. Справа № 760/12767/17. URL: http://www.reyestr.court.gov.ua/Review/69160909 (дата звернення: 23.07.2020).
13. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження). Сайт Верховної Ради України від 15.01.2020 р. № 2740. URL: http://www.reyestr.court.gov.ua/Review/59333908 (дата звернення: 23.07.2020).
14. Sammons J., Brunty J. Mobile device forensics: threats, challenges and future trends, Digital Forensics: Threatscape and Best Practices, Syngress, 2015. 182 p.
15. Good Practice and Advice Guide for Managers of e-Crime Investigation. URL: http://www.acpo.police.uk/documents/crime/2011/201103 CRIECI14.pdf (date of the application: 23.07.2020).
16. Перякина М. П., Унжакова С. В., Шишкина Н. Э. Процессуальные и криминалистические аспекты изъятия электронных носителей информации в свете защиты прав участников уголовного судопроизводства. *Сибирский юридический вестник.* 2019. № 3 (861–2019). С. 81–85.

References

1. Internet-trafik (mirovoy rynok) [Internet traffic (world market)]. Retrieved from https://www.tadviser.ru/index.phperevoda [in Russ.].
2. Casey, E., & Turnbull, B. (2011). Digital Evidence on Mobile Devices [Digital Evidence and Computer Crime]. Third Edition. ACADEMIC PRESS.
3. Klymchuk, M. P. (2020). Slidy kryminalnykh pravoporushen, uchynenykh iz vykorystanniam zasobiv stilnykovoho zviazku, y osoblyvosti yikh vyiavlennia. Aktualni pytannia vyiavlennia ta rozkryttia zlochyniv Natsionalnoiu politsiieiu: vitchyznianyi ta zarubizhnyi dosvid: mater. Mizhnar. nauk.-prakt. kruhloho stolu / (m. Kyiv, 19 liut. 2020 r.) [Traces of criminal offenses committed with the use of cellular communications, and features of their detection. Topical issues of detection and detection of crimes by the National Police: domestic and foreign experience: materials of the International scientific-practical round table]. Kyiv: Nats. akad. vnutr. sprav [in Ukr.].
4. Yablokov, N. P. (Ed.) (2005). Kriminalistika [Kriminology]. M.: Yurist' [in Ukr.].
5. Bessonov, A. A. O nekotoryh vozmozhnostyah sovremennoy kriminalistiki v rabote s elektronnymi sledami [On some of the possibilities of modern forensics in working with electronic traces]. DOI: 10.17803/2311-5998.2019.55.3.046-052 [in Ukr.].
6. Potapov, S. A., & Potapova, I. S. (2016). Ispolzovanie ekspertiz pri rassledovanii i raskrytii prestupleniy, sovershennyh s primeneniem sotovyh telefonov [The use of expertise in the investigation and disclosure of crimes committed with the use of cell phones]. *Sotsialno-ekonomicheskie protsessyi i yavleniya (Socio-economic processes and phenomena),* 11, 11, 155–161. DOI: 10.20310/1819-8813-2016-11-11-155-161 [in Ukr.].
7. Kapinus, O. S. (2016). Kriminologiya. Osobennaya chast [Kriminology: Special part]. M., Izdat. Yurayt [in Russ.].
8. Kryminalnyi protsesualnyi kodeks Ukrainy: Zakon Ukrainy vid 13.04.2012 № 4651-VI [Criminal Procedural Code of Ukraine: Law of Ukraine]. Retrieved from https://zakon.rada.gov.ua [in Ukr.].
9. Postanova Verkhovnoho sudu Ukrainy vid 09.04.2020. Sprava № 727/6578/17; № 51-4494km19 [Resolution of the Supreme Court of Ukraine of April 9, 2020]. Retrieved from https://verdictum.ligazakon.net/document/88749345?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress05 [in Ukr.].
10. Vyrok Selydivskoho miskoho sudu Donetskoii oblasti vid 02.03.2016. [Judgment of the Selidovo City Court of the Donetsk Region of March 2, 2016]. Retrieved from http://www.reyestr.court.gov.ua/Review/56200716 [in Ukr.].
11. Shylo, A. B. (2018). Otrymannia informatsii z vyluchenoi elektronnoi tekhniky yak sposib zbyrannia dokaziv: spirni pytannia praktychnoho pravozastosuvannia [Obtaining information on seized electronic equipment as a way to gather evidence: controversial issues of practical law enforcement]. *Naukovyi jurydychnyi zhurnal (Scientific legal journal),* 5, 172–179 [in Ukr.].
12. Ukhvala slidchoho suddi Solomianskoho raionnoho sudu m. Kyieva vid 20.09.2017. Sprava № 760/12767/17 [Decision of the Investigating Judge of the Solomyansky District Court of Kyiv of September 20, 2017]. Retrieved from http://www.reyestr.court.gov.ua/Review/69160909 [in Ukr.].
13. Proekt Zakonu pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy ta Kryminalnoho kodeksu Ukrainy (shchodo vdoskonalennia poriadku zastosuvannia okremykh zakhodiv zabezpechennia kryminalnoho provadzhennia) vid 15.01.2020 r. № 2740 [Draft Law on Amendments to the Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine (on improving the procedure for applying certain measures to ensure criminal proceedings)]. Retrieved from http://www.reyestr.court.gov.ua/Review/59333908 [in Ukr.].
14. Sammons, J., & Brunty, J. (2015). Mobile device forensics: threats, challenges and future trends, Digital Forensics: Threatscape and Best Practices, Syngress.
15. Good Practice and Advice Guide for Managers of e-Crime Investigation. Retrieved from http://www.acpo.police.uk/documents/crime/2011/201103 CRIECI14.pdf
16. Peryakina, M. P., Unzhakova, S. V., & Shishkina, N. E. (2019). Protsessualnyie i kriminalisticheskie aspektyi iz'yatiya elektronnyh nositeley informatsii v svete zaschity prav uchastnikov ugolovnogo sudoproizvodstva [Procedural and forensic aspects of the seizure of electronic media in the light of protecting the rights of participants in criminal proceedings]. *Sibirskiy yuridicheskiy vestnik (Siberian legal bulletin),* 3, 81–85 [in Russ.].

Стаття: надійшла до редакції 14.07.2020
прийнята до друку 21.09.2020

The article: is received 14.07.2020
is accepted 21.09.2020