MOBILE PHONE (SMARTPHONE) IS A SOURCE OF CRIMINALISTICS INFORMATION

Igor N. Gorbanov
Odesa State University of Internal Affairs, Ukraine
e-mail: gor-i-gor@ukr.net

Abstract: This article discusses a mobile phone (smartphone) as a source of forensic information. To understand the technology of wireless communications, a brief overview of the basic principles of the functioning of a telecommunication network is made. Based on the accumulated experience and scientific developments, typical traces are found that are on the surface of the device and its elements; stored in the memory blocks of the hardware-software complex of the device, as well as the inserted SIM-card and memory card; hosted on servers (in "cloud" information storage services), which can be accessed by authorization using a smartphone. The possibilities and directions of a possible expert and non-expert identification and study of the described traces are considered. The features of the current state of forensic support tactics for examining a mobile phone are highlighted, its problems are identified and proposals for their solution are formulated. The possibilities of national databases are analyzed, which contain the relationship between the personal data of the user, IMEI of his mobile phone (smartphone), numbers and contacts of the phone book, and more. The names and functional purpose of computer programs for searching and analyzing data, including remote data from mobile devices, are indicated.

Keywords: mobile phone, smartphone, trace, SIM-card, memory card, investigation, computer-technical examination.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасних умовах розвитку людської цивілізації засоби мобільного зв'язку, серед яких поважне місце займають мобільні телефони (смартфони), отримали широке розповсюдження. Так, знаходячись при власникові мобільні телефони (смартфони), як високотехнологічні продукти задовольняють багаточисленні потреби, дозволяючи оперативно та дистанційно вирішувати безліч завдань, серед яких: зв'язок з іншими абонентами, керування інтерактивними системами будинків, рухом транспортних засобів та безпілотних літальних апаратів, рахунками в банках (використовувати пристрій для оплати і отримання платежів), створення та зберігання різних видів інформації, відтворення текстових, графічних, аудіо- та відеофайлів, користування різними каналами інформації за допомогою мережі Інтернет (електронна пошта, месенджери та інші), а також проведення біржових операцій з купівлі/продажу цінних паперів у режимі реального часу, та багато інших. За арсеналом функцій у сучасних мобільних телефонів (смартфонів) більше спільного з комп'ютерами, ніж з аналоговими телефонами, що робить їх незамінними засобами для реалізації протиправних задумів та вельми корисними для забезпечення організованої злочинної діяльності.

Перебуваючи постійно при користувачеві мобільні телефони (смартфони) інколи виступають як засобом вчинення кримінального правопорушення (шахрайство, поширення шкідливого програмного забезпечення), так і його предметом (крадіжка). У ході проведення слідчих (розшукових) дій та оперативно-розшукових заходів для встановлення місцезнаходження безвісти відсутньої особи такі засоби мобільного зв'язку виступають відправною точкою, бо містять перелік останніх контактів, історію браузера зі згадками про останні інтернет-сайти, менеджери з переписками з іншими абонентами, відомості про фінансову активність та службові журнали з фіксацією з'єднань з певними стільниковими базовими станціями телекомунікаційної мережі. У зв'язку з цим мобільні телефони (смартфони) є джерелом криміналістично важливої інформації, яка при професійному виявленні, фіксуванні, аналізі та подальшому використанні зможе допомогти у вирішенні завдань охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [1].

Слідчі та оперативні працівники при затриманні кожного правопорушника або встановленні жертви злочину, у переважній більшості випадків, виявляють мобільний телефон (смартфон), що потенційно є цінним джерелом криміналістично важливих відомостей, однак при цьому зосереджуючись на одному виді слідової інформації можуть не помітити інші дані, що може унеможливити повне системне комплексне вивчення усіх обставин розслідуваної події. Це виключно негативно відобразиться на захисті особи, суспільства та держави від кримінальних правопорушень…, забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений…[2]. Вказане робить проблематику

розгляду мобільного телефону (смартфону) як джерела криміналістично значимої різноякісної та різноспрямованої інформації, вельми актуальною.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Проблематика особливостей та специфіки тактики огляду предметів-носіїв криміналістично значимої інформації давно притягує погляди вітчизняних і закордонних вчених-криміналістів. Серед тих, хто зробив значний внесок у вирішення цієї проблеми можна назвати: Т.В. Авер'янову, В.П. Бахіна, Р.С. Бєлкіна, П.Д. Біленчука, В.Б. Вєхова, М.С. Вертузаєва, А.Ю. Головіна, В.Г. Гончаренка, В.А. Журавля, А.В. Іщенка, О.Н. Колесніченка, В.В. Крилова, Є.С. Лапін, В.В. Лисенка, В.К. Лисиченка, І.М. Лузгіна, Г.А. Матусовського, М.В. Салтевського, М.Я. Сегая, В.С. Цимбалюка, В.Ю. Шепітька та інших. Вказані автори створили суттєве теоретичне підґрунтя для мобільних засобів зв'язку з криміналістичних позицій. Ураховуючи суцільне розповсюдження та широку практику використання смартфонів в аудіовізуальному та текстовому спілкуванні (передаванням даних і так далі), в тому числі за для здійснення злочинної діяльності, вчені-криміналісти не обминули своєю увагою доказовий потенціал таких засобів при розслідуванні окремих видів кримінальних правопорушень, чим надали істотну допомогу слідчій та оперативно-розшуковій практиці з протидії злочинам. Зазначимо, що спеціальних досліджень щодо мобільного телефону (смартфону), як джерела криміналістично значимої різноякісної інформації в Україні не проводилося. Низка існуючих криміналістичних досліджень вітчизняних авторів: К.О. Щераковської «Засоби мобільного зв'язку як джерела інформації при розслідуванні торгівлі дітьми» (2012 р.), О.В. Одерія, С.О. Корони, С.В. Самойлова «Тактика слідчого огляду комп'ютерних систем та їх елементів (2010 р.), Д.А. Морозова, В.С. Бондаря «Використання спеціальних знань під час проведення слідчих (розшукових) дій у розслідуванні незаконного посіву або вирощування снотворного маку чи конопель» (2017 р.), А.В. Коваленка «Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста» (2017 р.), М.В. Зубова «Особливості проведення першочергових слідчих (розшукових) та негласних слідчих (розшукових) ді під час розшуку безвісно відсутніх осіб» (2016 р.) є актуальними та повними, але, на нашу думку, лише фрагментарно висвітлюють загальну проблематику розгляду мобільного телефону (смартфону), як джерела криміналістично значимої різноякісної та різноспрямованої інформації. Вони надають лише уривчасте уявлення про наявність відомостей, котрі потенційно можуть отримати статус доказів, що негативно відображається на якості слідчої та оперативно-розшукової практики.

Формулювання цілей статті (постановка завдання). Розглянути мобільний телефон (смартфон) як джерело криміналістично значимої інформації; визначити типові сліди з означенням напрямів їх дослідження; висвітлити особливості сучасного стану криміналістичного забезпечення слідчого огляду мобільного телефону, встановити його проблематику та сформулювати пропозиції щодо їх вирішення.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Криміналістично значуща інформація, що міститься в засобах мобільного зв'язку, обумовлена їх технічними і функціональними особливостями [3, с. 1110]. Тож, для формування коректного уявлення про усю гамму слідової криміналістично значимої різноякісної та різноспрямованої інформації, яку потенційно можна отримати при огляді та аналізі відомостей мобільний телефон (смартфон), доцільно розібратися із загальними принципами роботи бездротового доступу такого приладу до телекомунікаційної мережі. Відповідно до положень Закону України «Про телекомунікації» мобільний зв'язок можна представити як електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру [4]. Під кінцевим обладнанням мається на увазі автономний мобільний телефон (смартфон), призначений для роботи в мережах стільникового зв'язку, що використовує приймач радіодіапазону і традиційну телефонну комутацію для здійснення телефонного зв'язку на території зони покриття мережі. Більшість пристроїв має свій унікальний номер IMEI - міжнародний ідентифікатор мобільного пристрою, що присвоюється при виробництві і складається, як правило, з 15 цифр. Цей унікальний код дозволяє ідентифікувати пристрій у мережі, відслідковувати переміщення, дзвінки та багато іншого. Більшість стандартів мобільного зв'язку використовують для ідентифікації абонента SIM-карту. Вона являє собою смарт-карту (пластикову картку з запресованої в неї мікросхемою мікроконтролера і пам'яті) з програмним управлінням, і також має свій унікальний номер IMSI (англ. International Mobile Subscriber Identity - міжнародний ідентифікаційний номер рухомого абонента) та індивідуальний цифровий пароль [5]. Наведений унікальний номер IMEI разом з номером SIM-карти абонента сприймається як ідентифікатор базовими станціями мобільного зв'язку.

Мобільний телефон (смартфон) є складним пристроєм, який складається з багатьох елементів, але, з криміналістичного боку, цікавими є лише слідовмісні та сприймаючі складові, у широкому розумінні

вказаного терміну. До таких ми відносимо: корпус (захисне скло та плівка, бампер, чохол, брелок), програмно-апаратний комплекс, SIM-картка та картка пам'яті.

Слідова картина, що міститься на/у мобільному телефоні (смартфоні), складається із:

1) слідів, що знаходяться на поверхні пристрою, а саме на корпусі, конструктивних частинах, захисному склі чи плівці, бампері, чохлі, брелку;

2) слідів, котрі зберігаються у блоках пам'яті програмно-апаратного комплексу пристрою, а також вставленій SIM-картці та картці пам'яті;

3) слідів, які зберігаються на серверах (у «хмарних» сервісах зберігання інформації), до яких можна отримати доступ (авторизуватись) за допомогою досліджуваного пристрою.

Перед тим, як почати розгляд наведеної класифікації слідів, що містяться на/у мобільному телефоні (смартфоні), доцільно вказати, що сам означений пристрій можна дослідити за допомогою товарознавчої експертизи і встановити його найменування, призначення та вартість; належність до класифікаційних категорій, які прийняті у виробничо-торговельній сфері [6]; та інше, у залежності від слідчої необхідності та обставин кримінального правопорушення.

Спираючись на практику підрозділів Національної поліції можна вказати, що сліди, які знаходяться на поверхні пристрою, а саме на корпусі, конструктивних частинах (елементі живлення), SIM-картці, картці пам'яті, захисному склі чи плівці, бампері, чохлі, брелку мають знайому широкому загалу природу походження та базові характеристики. Прикладом таких слідів можуть бути: а) сліди папілярних візерунків та вушної раковини, що утворені нашаруванням потожирової речовини, котрі можуть бути досліджені у ході дактилоскопічного (пороскопічного, еджеоскопічного) дослідження. Означені сліди, а також сліди слини, у області мікрофона, можуть бути досліджені геномною (ДНК) експертизою, при дотриманні відповідної процедури отриманні зразків, що виключить «забруднення»; б) сліди нашарування косметичних засобів (губна помада, блиск, пудра, тональний крем, рум'яна), що можуть бути досліджені під час проведення експертизи матеріалів, речовин та виробів; в) трасологічні сліди, зокрема, характерні подряпини від каблучок чи сліди автомобільного тримача при утриманні мобільного телефону (смартфону), можуть бути досліджені трасологічною експертизою.

Співробітники органів правопорядку знайомі з можливостями отримання криміналістичної інформації з SIM-картки (абревіатура від англ. subscriber identification module) – ідентифікаційний модуль абонента у вигляді смарт-карти, що застосовується в мобільному зв'язку. Ідентифікація такої карти здійснюється за допомогою алгоритму та таємного PIN-коду, які записані на карті, крім ідентифікації карта служить для дешифрування голосу та телекомунікаційних сигналів, де зберігається певна кількість контактних даних абонентів, а також частина отриманих та відправлених SMS-повідомлень. При дослідженні SIM-картки необхідно пам'ятати про обмежену кількість звернень при отриманні доступу до її даних. Після правильного введення PIN-коду (у разі його незнання – PUK1-коду) всі функції разом з інформаційним наповненням SIM-карти стають доступними одразу після включення і завантаження телефону [7]. Це доцільно враховувати при прийнятті рішення про виключення мобільного телефону (смартфону) у ході його огляду, пакування та вилучення. У теперішній час SIM-картки витісняються віртуальною карткою eSIM, що емулюється мікросхемою, яка додається безпосередньо в пристрій на етапі його виробництва. Вона не може бути замінена, для внесення змін або використання профілю потрібно вводити пароль, що суттєво ускладнює користування вкраденим телефоном та полегшує його виявлення [8].

В Україні процедура набуття номера обраного мобільного оператора через купівлю SIM-картки не передбачає якоїсь ідентифікації особи за паспортом, що сприяє анонімності при використанні мобільного телефону у вчиненні злочинів, і відповідно, утруднює подальшу роботу з їх розслідування.

При огляді мобільного телефону (смартфону) затриманої особи, що займається протиправною діяльністю, правоохоронці, як правило, стикаються з тим, що контактні дані абонентів записані у вигляді прізвиська, абревіатури, імені, котрі не надають достатньої інформації для їх ідентифікації. У національних правоохоронних органів існує потенційна оперативна можливість встановлення істинних персональних даних за допомогою бази «Антарес». Відомості у згаданій базі містять зв'язки між анкетними даними користувача, IMEI його мобільного телефону (смартфону), номерами та іменами контактів телефонної книги та інше. З власного досвіду зазначимо, що обсяг роботи для наповнення бази «Антарес» важко порівнювати з ефектом від її використання, що обумовлює розгляд напрямів для збільшення продуктивності.

У теперішній час певне розповсюдження отримали комерційні мобільні додатки з Google Play, що допомагають в ідентифікації користувачів мобільних номерів, наприклад, NumBuster (Gilraen Limited), Getcontact (Getverify LDA), Eyecon (Eyecon Phone Dialer & Contacts) та інші. Результативність вказаних програм потребує окремого дослідження, проте окремі поліцейські у професійній діяльності користуються усіма можливими засобами для встановлення особи невідомого абонента з телефонної книги певної SIM-картки.

З розвитком технологій фото- та відеозйомки, а також зі збільшенням обсягів циркулюючої інформації досліджувані пристрої змушені використовувати додаткові засоби для збереження даних,

зокрема карти пам'яті. Вони є компактними електронними носіями інформації, що використовуються для зберігання цифрової інформації [9]. Як правило, операційна система мобільного телефону (смартфону) самостійно розміщує на карті пам'яті програмні продукти, сервісні службові файли, аудіо-, фото-, відеофайли, текстові та графічні файли, каталоги з файлами месенжерів соціальних мереж, та інше. Тому, слідчий та спеціаліст за допомогою сертифікованого службового обладнання, з використанням ліцензійного програмного забезпечення, може провести огляд скопійованої інформації карти пам'яті. Якщо ж носій захищено будь-яким типом захисту від зчитування чи копіювання, слід призначити судову комп'ютерно-технічну експертизу та поставити перед експертом питання про можливість отримання доступу до вмісту такого носія [10, с. 182-191]. У подальшому після успішного отримання файлів зі згаданого носія можна провести експертизу відеозвукозапису та інші дослідження, а також необхідні слідчі (розшукові) дії.

Сліди, що зберігаються у блоках пам'яті програмно-апаратного комплексу пристрою, тобто самого мобільного телефону (смартфону) є найменш вивченими криміналістами, і відповідно, найменш використовуваними у якості доказів.

По-перше, у якості доказової інформації можна розглядати список бездротових точок доступу – радіомереж формату Wi-Fi, до яких раніше під'єднувався досліджуваний пристрій. Така точка доступу є сполучною ланкою з'єднання дротового і бездротового сегментів мережі, і має наступні важливі для доказування характеристики: 1) знаходячись на краю мережевого дроту вона має свою унікальну IP-адрес, за якою через провайдера інтернет-послуг можна встановити географічні координати та фізичне розміщення (адреса); 2) точка доступу має назву, що вноситься до реєстру доступних мереж Wi-Fi у налаштуваннях мобільного телефону (смартфону) особи, що вчинила кримінальне правопорушення. Вказані технічні передумови та потреби слідчих підрозділів обумовили появу постійно оновлюваної бази мереж Wi-Fi в Україні, за допомогою якої, за наявності назви точки доступу Wi-Fi, можна встановити перебування мобільного телефону (смартфону) разом із власником за певною фактичною адресою (місто, вулиця, будинок, квартира).

По-друге, кожен мобільний телефон (смартфон) має внутрішню пам'ять, яка складається з видимої для користувача частини, де він розміщує необхідне програмне забезпечення, фотографії і так далі, а також невидимої та недоступної для власника пам'яті, що забезпечує штатну роботу операційної системи, блоків зв'язку та іншого. У цій «невидимій» частині є службові протоколи, що містять записи про усі з'єднання з базовими станціями. У теперішній час у вільному доступі знаходяться дані щодо елементів мережі базових станцій операторів мобільного зв'язку, за якими за допомогою вихідних даних з телефона, за необхідності, можна побудувати приблизний маршрут його користувача.

Також слід вказати на особливості роботи внутрішньої пам'яті мобільного телефону (смартфону) при обслуговуванні месенджерів соціальних мереж, серед яких: Viber, WhatsApp, Telegram, Skype, Facebook Messenger. У багатьох з наведених месенджерів є функції з видалення бесід, чатів, мультимедійних повідомлень. Однак, видалена інформація та окремі файли не піддаються фізичному видаленню і знаходяться у недоступній для користувача частині внутрішньої пам'яті. Для відновлення видаленої таким чином інформації спеціалісти застосовують повне копіювання усієї внутрішньої пам'яті мобільного телефону (смартфону), шляхом створення її образу. Для таких дій використовуються наступні програмні продукти:

- Cellebrite UFED 4PC Ultimate включає в себе UFED Physical Analyzer для глибокого декодування, аналізу та підготовки звітів (витяг на фізичному рівні і декодування отриманих даних з обходом блокування введення графічного ключа / пароля / PIN-коду з пристроїв Android…);

- лінійка програмних продуктів компанії MSAB: XRY (відновлення даних з мобільних пристроїв), XAMN (створення образу та подальшого аналізу даних зі смартфону) та інші, частина з яких є безкоштовною і може використовуватися самостійно слідчими та оперуповноваженими [11];

- для аналізу та візуалізації даних для ефективної аналітики IBM i2 Analyst's Notebook 9.0.

Мобільний телефон (смартфон) можна розглядати як засіб для отримання доступу до слідової криміналістично важливої інформації, що зберігається на серверах, що позиціонуються як «хмарні сховища» - модель схову даних, де цифрові дані зберігаються в логічні пули, а фізичне зберігання охоплює кілька серверів [12]. Серед популярних сервісів хмарного зберігання даних можна назвати український eDisk Ukr.net, американські GoogleDrive, DropBox, російські Яндекс Диск, Диск Mail.ru тощо [10, с. 182-191]. Отже, серед імовірних варіантів доступу до подібних сховищ та інших систем можна вказати на: 1) отримання доступу до електронних скриньок з наперед набраним паролем, бо шлях доступу сприймається як традиційний; 2) отримання доступу до сторінок у соціальних мережах, де можна з правами власника побачити повну інформацію про коло контактів, переписки зі спільниками і так далі; 3) отримання доступу до електронних платіжних систем «Qiwi Wallet», «WebMoney», а також до серверів підтримки різного виду криптовалют; 4) отримання доступу до «хмарного» сховища контактів [13, с. 216-222]; 5) отримання

доступу до різноманітних сайтів з правами зареєстрованого клієнта, наприклад, на сторінки інтернет-магазинів з продажу наркотичних засобів чи іншого. Наведені варіанти віддаленого доступу об'єднує авторизація в акаунтах подібних сервісів за допомогою мобільного телефону (смартфону).

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку. Мобільний телефон (смартфон) є унікальним джерелом криміналістично значимої різноякісної та різноспрямованої інформації, яка при кваліфікованому обізнаному підході може суттєво допомогти у проведенні розслідування кримінального правопорушення. Виявлення, фіксація та аналіз комплексу слідів, що знаходяться на поверхні частин згаданого пристрою; зберігаються у блоках його пам'яті, SIM-картці, картці пам'яті, «хмарних» сервісах (з авторизацією та подальшим доступом) – допоможе встановити обставини, які підлягають доказуванню у кримінальному провадженні.

References:

1. Zakon Ukrayini «Pro Natsionalnu politsiyu» vid 2 lipnya 2015 roku № 580-VIII [Law of Ukraine «On the National Police» of July 2, 2015. № 580-VIII]. Available at: https://zakon.rada.gov.ua/laws/show/580-19. (In Ukrainian).

2. Kriminalniy protsesualniy kodeks Ukrayini vid 13.04.2012 № 4651-VI [Criminal procedure code of Ukraine of 13.04.2012 № 4651-VI]. Available at: http://zakon3.rada.gov.ua/laws/show/4651-17 (accessed 19.12.2019). (In Ukrainian).

3. Scherbakovska, K.O. (2012) Zasobi mobilnogo zv'yazku yak dzherela informatsiyi pri rozsliduvanni torgivli ditmi [Mobile communications as a source of information in the investigation of child trafficking] // Forum prava [Forum of Law], 2012, № 1, 1109-1113. Available at: http://www.nbuv.gov.ua/e-journals/FP/2012-1/12skortd.pdf (accessed 19.12.2019). (In Ukrainian).

4. Zakon Ukrayini «Pro telekomunikatsiyi» 18 listopada 2003 roku № 1280-IV [Law of Ukraine «On Telecommunications» November 18, 2003 № 1280-IV] Available at: https://zakon.rada.gov.ua/laws/show/1280-15 (accessed 19.12.2019). (In Ukrainian).

5. Mobilniy telefon [Cellphone]. Available at: https://uk.wikipedia.org/wiki/Мобільний_телефон (accessed 19.12.2019). (In Ukrainian).

6. Nakaz Ministerstva yustitsiyi Ukrayini vid 08.10.98 № 53/5 «Pro zatverdzhennya Instruktsiyi pro priznachennya ta provedennya sudovih ekspertiz ta ekspertnih doslidzhen ta naukovo-metodichnih rekomendatsiy z pitan pidgotovki ta priznachennya sudovih ekspertiz ta ekspertnih doslidzhen» [Order of the Ministry of Justice of Ukraine dated 08.10.1998 № 53/5 «On approval of the Instruction on appointment and conduct of forensic examinations and expert research and Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert research»] Available at: https://zakon.rada.gov.ua/laws/show/z0705-98 (accessed 19.12.2019). (In Ukrainian).

7. SIM-kartka [SIM-card]. Available at: https://uk.wikipedia.org/wiki/SIM-картка (accessed 19.12.2019). (In Ukrainian).

8. ESIM [ESIM]. Available at: https://uk.wikipedia.org/wiki/ESIM (accessed 19.12.2019). (In Ukrainian).

9. Karta pam'yati [Memory card]. Available at: https://uk.wikipedia.org/wiki/карта пам%яті (accessed 19.12.2019). (In Ukrainian).

10. Kovalenko, A.V. (2017) Osoblivosti taktiki oglyadu elektronnih dokumentiv pid chas dosudovogo rozsliduvannya posyagan na zhittya ta zdorov'ya zhurnalista [Peculiarities of electronic document review tactics during the pre-trial investigation of encroachments on the life and health of a journalist] // Visnik Natsionalnoyi akademiyi pravovih nauk Ukrayini [Bulletin of the National Academy of Legal Sciences of Ukraine], № 1 (88), 2017, P. 182-191 (In Ukrainian).

11. Laboratoriya komp'yuternoyi kriminalistiki EPOS [Computer Forensics Laboratory EPOS]. Available at: https://www.epos.ua/view.php/index (accessed 19.12.2019). (In Ukrainian).

12. Hmarni shovischa [Cloud storage]. Available at: https://uk.wikipedia.org/wiki/Хмарні_сховища (accessed 19.12.2019). (In Ukrainian).

13. Morozov, D.A., Bondar, V.S. (2017) Vikoristannya spetsialnih znan pid chas provedennya okremih slidchih (rozshukovih) diy u rozsliduvanni nezakonnogo posivu abo viroschuvannya snotvornogo maku chi konopel [Use of special knowledge during certain investigative (search) actions in the investigation of illegal sowing or cultivation of sleeping poppy or hemp] // Visnik NTUU «KPI». Politologiya. Sotsiologiya. Pravo [Bulletin of National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute». Politology. Sociology. Right], № 1/2 (33/34), 2017, P. 216-222. (In Ukrainian).

Мобильный телефон (смартфон) как источник криминалистически значимой информации

Горбанёв Игорь Николаевич, e-mail: gor-i-gor@ukr.net
Одесский государственный университет внутренних дел, г. Одесса, Украина

Аннотация: В предлагаемой статье рассматриваются мобильный телефон (смартфон) как источник криминалистически значимой информации. Для понимания технологии беспроводной связи выполнен краткий обзор основных принципов функционирования телекоммуникационной сети. На основе накопленного опыта и научных разработок определены типичные следы, находящиеся на поверхности устройства и его элементах; хранящиеся в блоках памяти программно-аппаратного комплекса устройства, а также вставленной SIM-карте и карте памяти; размещенные на серверах (в «облачных» сервисах хранения информации), к которым можно получить доступ путем авторизации с помощью смартфона. Рассмотрены возможности и направления возможного экспертного и неэкспертного выявления и исследования описанных следов. Освещены особенности современного состояния криминалистического обеспечения тактики осмотра мобильного телефона, установлена его проблематика и сформулированы предложения по их решению. Проанализированы возможности национальных баз данных, которые содержат связи между анкетными данными пользователя, IMEI его мобильного телефона (смартфона), номерами и именами контактов телефонной книги и прочее. Указаны наименования и функциональное назначение компьютерных программ для поиска и анализа данных, в том числе и удалённых, из мобильных устройств.

Ключевые слова: мобильный телефон, смартфон, следовая картина, SIM-карта, карта памяти, следственный осмотр, компьютерно-техническая экспертиза.