Кобець Микола Вікторович,
доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС «CELLEBRITE UFED» ЯК ЗАСІБ ОТРИМАННЯ ІНФОРМАЦІЇ З МОБІЛЬНИХ ТЕРМІНАЛІВ

Сучасні інноваційні досягнення, технологічні та програмно-технічні рішення значно розширюють можливості правоохоронних органів, надаючи їм усі необхідні інструментарії для отримання (вилучення) процесуально значущих даних із електронних (інформаційних) засобів та систем, які значно скорочують час проведення слідства, уніфікують дії правоохоронців, що у подальшому сприяє успішному доведенню справи до суду.

У цьому контексті до одного із сучасних технічних нововведень можна віднести апаратно-програмний комплекс «Cellebrite UFED», що активно використовується правоохоронцями під час здійснення заходу зі зняття інформації з електронних інформаційних систем (мереж), а також під час процесуальних дій.

Для вирішення питань з отримання даних із електронних (інформаційних) комунікаційних засобів ізраїльська компанія «Cellebrite Ltd.» (סלברייט) розробила інноваційний комплекс «Cellebrite» для вилучення (копіювання) криміналістично (оперативно-розшукової) значимої інформації для правоохоронних органів, призначений для вилучення даних з таких мобільних терміналів як стільникові радіотелефони з тастатурним (кнопковим) набором, смартфонів, ай-фонів, планшетів, переносних GPS-трекерів, безпілотних літальних апаратів тощо для подальшого розшифрування та аналізу.

Апаратно-програмний комплекс «Cellebrite UFED» за допомогою програмного забезпечення вилучає (копіює) із мобільного терміналу, зокрема, стільникового радіотелефону важливі для правоохоронних органів дані, які у подальшому можуть допомогти правоохоронцям встановити факти причетності особи до вчинення кримінального правопорушення, наприклад, телефоні книги, фотографії, відеозаписи, текстові повідомлення, журнали викликів, дані ESN і IMEI, а згодом збирає дані у електронний звіт для проведення досліджень і збору доказів.

Також його застосування надає можливість доступу до «хмарних» сховищ інформації за допомогою вилучених з мобільного терміналу (стільникових радіотелефонів) тимчасових ключів авторизації, відновлення видаленої інформації, у тому числі фотоматеріалів, побудови маршрутів пересування шляхом аналізу історії використання точок доступу до Wi-Fi роутерів тощо.

Цей технічний пристрій може зчитувати інформацію з таких мессенджерів як Viber, WhatsApp, Telegram тощо.

Рис. 1 Апаратно-програмний комплекс «Cellebrite UFED Touch 2 Ultimate»

У структурі МВС України ці комплекси знаходяться на обслуговувані оперативно-технічних підрозділів Національної поліції України, експертної служби ДНДЕКЦ МВС України. 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».

Ці апаратно-програмні комплекси правоохоронними органами використовуються у межах:

- проведення такої слідчої (розшукової) дії як огляд місцевості, приміщення, речей, документів та комп'ютерних даних (стаття 237 КПК України «Огляд») для огляду мобільного терміналу (стільникового радіотелефону) та/або SIM-картки виявленого на місці вчинення кримінального правопорушення;

- кримінального провадження під час проведення такої слідчої (розшукової) дії як обшук житла чи іншого володіння особи, обшуку особи (стаття 236 КПК України «Виконання ухвали про дозвіл на обшук житла чи іншого володіння особи») для доступу до комп'ютерних систем або їх частин, мобільних терміналів (стільникових радіотелефонів) та/або SIM-карток;

- оперативно-розшукових справ та/або кримінальних проваджень під час проведення відповідних оперативно-технічних заходів та негласних слідчих (розшукових) дій зі зняття інформації з електронних інформаційних систем (згідно до частини 2 статті 8 Закону України «Про оперативно-розшукову діяльність» та статті 264 КПК України), які здійснюють на підставі ухвали слідчого судді про дозвіл на проведення відповідного заходу.

Зазвичай до зазначених дій слідчий залучає працівника оперативно-технічного підрозділу, як спеціаліста, згідно статті 71 КПК України. При цьому відповідно до пункту 1 частини 5 статті 71 КПК України спеціаліст при прибутті за викликом слідчого, дізнавача, прокурора, суду повинен мати при собі необхідні технічне обладнання, пристрої та прилади. Тому слідчий інформує з місця події свого керівника про необхідність залучення відповідного спеціаліста з апаратно-

програмним комплексом «Cellebrite UFED». Участь працівника оперативно-технічного підрозділу слідчий фіксує у протоколі огляду предмета. Працівник оперативно-технічного підрозділу на місці події у присутності понятих за допомогою апаратно-програмного комплексу «Cellebrite UFED» здійснює огляд комп'ютерних даних виявленого та вилученого з місця події слідчим стільникового радіотелефону, тобто його інформації, та створює «образ»/електронний звіт наявної інформації. Створений «образ»/електронний звіт спеціаліст записує на цифровий диск на зразок CD-R, DVD-R у виді файлу, закріплює електронною міткою у виді контрольної суми (hesh symma) з використанням алгоритму SHA-1, SHA-2 або MDS. Зафіксовану інформацію на цифровому диску особа, яка здійснює ці процесуальні дії, також засвідчує електронним підписом. Відповідно до законодавства України у сферах електронних довірчих послуг та електронної ідентифікації [3], а також зважаючи на позицію, витлумачену Верховним Судом [1], електронний підпис прирівняно до власноручного.

Огляд комп'ютерних даних проводиться слідчим, прокурором, відображаючи у протоколі огляду інформацію, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі), згідно частини 2 статті 237 КПК України.

За результатами огляду слідчий складає протокол згідно статті 104 КПК України. До протоколу як додаток долучається стільниковий радіотелефон, матеріальний носій інформації, підписаний працівником оперативно-технічного підрозділу алгоритмом хешування SHA-1, SHA-2 або MDS, з відомостями отриманими під час огляду інформації мобільних терміналів (стільникових радіотелефонів) та/або SIM-карток (стаття 105 КПК України). Згідно із частиною 5 статті 104 КПК України протокол підписують всі учасники, які брали участь у проведенні процесуальної дії.

Розглядаючи протокольне оформлення доказової бази слід зауважити, що у статті 84 КПК України зазначено, що джерелами доказів є показання, речові докази, документи, висновки експерта. Згідно пункту 1 частини 2 статті 99 КПК України до документів можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані).

Список використаних джерел

1. Верховний Суд. Касаційний господарський суд. (2021, січень 29). Про стягнення коштів у сумі 525 736,50 грн : постанова у справі № 922/51/20.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 року № 4651-VI.

3. Про електронні довірчі послуги : Закон України 05.10.2017 № 2155-VIII.

4. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами

Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575.

5. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГПУ, МВС, СБУ, АДПС, МФ, МЮ України від 16.11.2012 № 114/1042/516/1199/936/1687/5.

6. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. № 2135–XII // ВВРУ, 1992. № 22. Ст. 303.

7. Спеціальна техніка: основні поняття, терміни та визначення : навчальний посібник / М.В. Кобець, Б.В. Жуков, П.П. Артеменко. Київ : Аванпост-Прим, 2013. 192 с.

Козій Василь Васильович,
докторант кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук

КОПІЮВАННЯ, АРХІВУВАННЯ ТА ГЕШУВАННЯ ФАЙЛІВ ПРИ ЗДІЙСНЕННІ ФІКСАЦІЇ ДАНИХ З МЕРЕЖІ «ІНТЕРНЕТ» ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ КРИПТОВАЛЮТ

Починаючи із появи у 2008 році першої у світі криптовалюти біткоїна, і по наш час відбувся бурхливий розвиток криптовалют. Наразі ринок криптовалют являє собою десятки, якщо не сотні тисяч ресурсів, які надають можливість будь-кому, практично в бідь-якій точці світу, всього за декілька хвилин за допомогою грошових коштів із банківської карти придбати ту чи іншу криптовалюту, NFT-токени, або стейблкоїни. Так, відповідно до даних ресурсу CoinMarketCup, станом на 16.03.2023 на ньому наявна інформація про 22 940 криптовалют та 5870 онлайн бірж, на яких здійснюється торгівля криптовалютою, а капіталізація ринку криптовалют становить понад трильйон доларів США, при цьому добовий обсяг торгів перевищує 78,5 мільярди доларів США [1].

Ресурс Coin Geko станом на 16.03.2023 містить інформацію про 11 393 монети, які на ньому відстежуються [2].

У багатьох країнах світу криптовалюта стала звичним явищем у житті мільярдів людей.

В Україні криптовалюту законодавцем віднесено до віртуальних активів. Так, 17.02.2022 ухвалено Закон України «Про віртуальні активи», який проте до цього часу не набрав чинності. Згідно з п. 1 указаного Закону віртуальний актив – це нематеріальне благо, що є об’єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі [3].