МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ЗАСТОСУВАННЯ АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ «CELLEBRITE UFED» ПІД ЧАС ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Методичні рекомендації

Київ – 2023

УДК 343.98 : 343.132 : 351.746.2
З-366

Матеріали схвалено науково-методичною радою Національної академії внутрішніх справ від 24 травня 2023 р., протокол № 9.

Розробники:
Тіхонов Сергій Васильович – завідувач кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, доктор філософії у галузі права, генерал поліції третього рангу;
Кобець Микола Вікторович – доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник.

Технічний консультант Колесник А. – старший оперуповноважений Департаменту оперативно-технічних заходів НП України, лейтенант поліції.

Застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень : методичні рекомендації. Київ : Національна академія внутрішніх справ, 2023. 41 с.

У методичних рекомендаціях розроблено алгоритм застосування апаратно-програмного комплексу «Cellebrite UFED» під час виявлення, припинення та розслідування кримінальних правопорушень.

Складається з чотирьох розділів і містять основні відомості із загальних понять, тактико-технічних можливостей апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень, порядку документування заходу із зняття інформації з електронних інформаційних систем (мереж) у межах якої застосовуються ці комплекси та особливостей документування процесуальних дій апаратно-програмним комплексом «Cellebrite UFED», пов’язаних із обшуком приміщень, осіб та оглядом мобільних терміналів.

Призначено для працівників органу досудового розслідування та оперативних підрозділів Національної поліції України. Методичні матеріали можуть бути корисним для науково-педагогічних працівників та науковців правоохоронних органів України.

© С.В. Тіхонов, М.В. Кобець 2023
© Національна академія внутрішніх справ

ЗМІСТ

1. Загальні положення

Сучасні комп'ютери та інші електронні технології, що можуть накопичувати, зберігати, аналізувати, кодувати і декодувати інформацію у чималих обсягах дедалі активніше перетворюються на могутній і водночас вразливий інструмент, за допомогою якого може здійснюватися збирання, а також поширення інформації. З розвитком інформаційних систем, електронних комунікаційних мереж збільшується кількість їх користувачів, а отже й мобільних терміналів, зокрема стільникових радіотелефонів (девайсів), більшають обсяги та підвищується складність даних, які зберігаються на цих пристроях. Зазвичай у стільникових радіотелефонах зберігається значний обсяг інформації, що пов'язаний з повсякденною життєдіяльністю людини.

У зв'язку з цим для з'ясування обставин вчинення кримінального правопорушення та встановлення істини у кримінальному проваджені постає нагальна потреба в отримані даних з електронних інформаційних пристроїв та систем. Це пов'язано з тим, що злочинці стали більше використовувати сучасні інформаційні та комп'ютерні технології у своїй протиправній діяльності. Для вирішення цієї потреби з ефективного виявлення та розслідування відповідних кримінальних правопорушень та враховуючи сьогодення законодавець ввів у кримінальний процесуальний кодекс такі слідчі (розшукові) дії як зняття інформації з електронних інформаційних систем та обстеження на місці події мобільних терміналів.

Зняття інформації з електронних інформаційних систем – заходи, що полягають в доступі до інформації електронних інформаційних систем (установленні їх логічного або фізичного місцезнаходження, програмному проникненні до них та/або встановленні безпосереднього фізичного/технічного контакту з ними та відборі інформації за визначеними ознаками), в отриманні інформації з електронних інформаційних систем або їх частин (копіюванні, знятті, передачі, фіксації та обробки), а також в інших діях із зазначеною інформацією (порушенні цілісності, знищенні або блокуванні).

Основне завдання проведення заходу із зняття інформації з електронних інформаційних систем полягає в забезпеченні конфіденційності доступу до комп'ютера фігуранта, інформаційно-комунікаційних засобів, носіїв інформації та виключення програмних можливостей операційної системи реєстрації дій працівника, який безпосередньо здійснює такі дії (час входу користувача в систему, журнал реєстрації дій користувача, журнал реєстрації підключення зовнішніх USB-приладів, журнал дій системи з передачі даних від одного пристрою до іншого, а також всередині системи під час зняття інформації з електронної системи фігуранта).

Для здійснення таких дій правоохоронці застосовують значний перелік спеціальних технічних засобів, спеціалізованих технічних пристроїв та спеціальне програмне забезпечення.

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

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

Апаратно-програмний комплекс «Cellebrite» серії «UFED» (з англ. Universal forensic extraction device), який застосовується правоохоронними органами, використовується у межах:

- оперативно-розшукових справ (далі – ОРС) та кримінальних проваджень під час проведення відповідних оперативно-технічних заходів (далі – ОТЗ) та негласних слідчих (розшукових) дій (далі – НСРД) 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;

- 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.

2. Тактико-технічні можливості апаратно-програмного комплексу «Cellebrite UFED» під час виявлення та розслідування кримінальних правопорушень

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 інших слідчих (розшукових) дій.

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 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.

Головні можливості апаратно-програмного комплексу «Cellebrite UFED»:

глибокий аналіз на фізичному рівні і на рівні файлової системи, логічне вилучення даних;

підтримка понад 40 000 моделей мобільних пристроїв;

підтримка таких операційних систем, як Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile і Palm OS;

клонування ідентифікатора SIM-картки, що дозволяє витягувати дані телефону, не допускаючи підключення мобільного терміналу до мережі;

вилучення даних з мобільного терміналу за допомогою кабельного підключення або безпроводового з'єднання Bluetooth;

вилучення даних з дронів виробництва компанії DJI;

вилучення даних з USB накопичувачів та карток пам'яті.

Для отримання інформації з мобільних терміналів підрозділи Національної поліції України, зокрема оперативно-технічні, активно використовують такі апаратно-програмні комплекси як «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC Physical Analyzer».

Розглянемо апаратно-програмний комплекс «Cellebrite UFED Touch 2 Ultimate» (див. рис. 1).

Технічні характеристики апаратно-програмного комплексу такі: процессор типу E3845; пам'ять SODIMM DDR3L: 8 Гб; екран емкісний мультитач, 5 точек; жосткий диск типу SSD 128 Гб; Wi-Fi 1T1R b/g/n/ac (~350 Мбит/с); акумулятор з'ємний, 4 ячейки, Li-Ion, 5000 мА-ч; розподільна здатність екрану 1024x600; Bluetooth подвійний режим 4.0/3.0; 4 порти USB 3.1, 1 фаза, 1,5 А на порт, часткова підтримка BC1.2; мультисім-рідер SIM, Micro SIM, Nano SIM; картридер SD, SDHC, SDXC, MMC; розміри 223 x 133 x 61 мм.

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

Види вилучення апаратно-програмним комплексом «Cellebrite UFED Touch 2 Ultimate»:

логічне вилучення – містить в себе вилучення різних типів даних, таких як журнали викликів, записи телефонної книги, текстові повідомлення SMS, MMS, електронні листи, події календаря, мультимедійні файли (зображення, відео тощо) та багато іншого;

вилучення SIM-даних – вилучення інформації з SIM-картки або USIM-картки;

вилучення файлової системи – повне вилучення пам'яті з телефону;

клонування SIM-картки – копіює ідентифікатор SIM-картки з однієї SIM-картки на іншу SIM-картку;

фізичне вилучення – використовує розширені методи для вилучення фізичного бітового зображення флеш-пам'яті мобільного терміналу, включаючи нерозподілений простір. На відміну від звичайних логічних процесів вилучення, фізичне вилучення обходить операційну систему мобільного терміналу і витягує дані з внутрішньої флеш-пам'яті телефону, нерозподілений простір може містити видалені елементи, такі як SMS, журнали викликів, записи телефонної книги, зображення, відео та аудіофайли;

використання камери UFED для фотографування або відеозапису пристрою.

Розглянемо апаратно-програмний комплекс «Cellebrite UFED 4 PC Physical Analyzer», що застосовується під час виявлення, припинення та розслідування кримінальних правопорушень (див. рис. 2).

Рис. 2 Апаратно-програмний комплекс «Cellebrite UFED 4 PC Physical Analyzer»

Апаратно-програмний комплекс «Cellebrite UFED 4 PC Physical Analyzer» має такі функціональні та технічні можливості:

вилучення на фізичному рівні та декодування отриманих даних з обходом блокування введенням графічного ключа /пароля/PIN-коду з пристроїв Android, враховуючи моделі Samsung Galaxy S, LG, HTC, Motorola та інші;

вилучення на фізичному рівні та лише на рівні файлової системи, а також декодування даних із пристроїв на базі Android із версіями ОС 4.2 – 4.4.3;

вилучення на фізичному рівні з пристроїв BlackBerry® на ОС 4 – 7;

ексклюзивне декодування: дані BBM, додатків, електронної пошти, Bluetooth та інше;

широка підтримка вилучення та декодування з пристроїв Apple;

вилучення на фізичному рівні та декодування із заблокованих пристроїв Nokia BB5 – вилучення пароля з вибраних пристроїв;

простий та швидкий доступ до заблокованих пристроїв шляхом обходу, відкриття або відключення коду блокування користувача;

витяг на фізичному рівні та декодування даних із пристроїв Windows Phone на базі ОС 8.0 – 8.1;

вилучення на рівні файлової системи з будь-яких пристроїв Windows Phone, HTC, Samsung, Huawei та ZTE;

відновлення різних типів віддалених даних з нерозподіленого простору в флеш-пам'яті пристрою;

декодування даних вилучення на фізичному рівні JTAG з великої кількості різних типів даних;

дешифрування журналу поетапного реєстрації TomTom® та вилучення даних з інших переносних пристроїв GPS;

дешифрування зашифрованої бази даних історії WhatsApp;

значний вибір варіантів декодування: дані програм, паролі, електронна пошта, журнал дзвінків, SMS, контакти, календар, мультимедійні файли, інформація про розташування тощо;

можливість комплексного аналізу через UFED Physical Analyzer, включаючи хронологію, аналітику проекту, виявлення шкідливого ПЗ та списки відстеження;

зручний генератор звітів у різних форматах за допомогою UFED Physical Analyzer;

переклад контенту іноземними мовами, міститься у даних, отриманих під час вилучення, за допомогою системи офлайнперекладу, що входить до UFED Physical Analyzer.

3. Особливості документування процесуальних дій апаратно-програмним комплексом «Cellebrite UFED», пов’язаних із обшуком приміщень, осіб та оглядом мобільних терміналів.

Проведення слідчих (розшукових) дій на місці події здійснюється із метою виявлення, оцінювання та дослідження слідів кримінального правопорушення, інших речей, що містять джерело доказової інформації, з’ясування обстановки кримінального правопорушення та інших обставин, що мають значення для кримінального провадження. При цьому слідчий застосовує наявний арсенал науково-технічних досягнень, оскільки він несе відповідальність за перебіг досудового розслідування.

У разі виявлення та вилучення мобільних терміналів на місці події слідчий ініціює застосування апаратно-програмного комплексу «Cellebrite UFED», який використовують у межах таких процесуальних дій:

- 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;

- 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.

Розглянемо ці напрями докладніше.

Після надходження до органу, підрозділу поліції інформації про вчинення кримінального правопорушення та внесення інформації до Єдиного реєстру досудових розслідувань (далі – ЄРДР) під керівництвом начальника органу, підрозділу поліції здійснюється комплекс першочергових заходів та невідкладних слідчих (розшукових) дій, у тому числі за дорученням слідчого, спрямованих на встановлення особи, яка вчинила кримінальне правопорушення, та з'ясування всіх обставин події.

Якщо на місці події був виявлений стільниковий радіотелефон, або на місці події перебувала чи була затримана особа, що підозрюють у вчинення кримінального правопорушення і у неї виявлений мобільний термінал слідчий у складі слідчо-оперативної групи (далі – СОГ) на місці вчинення кримінального правопорушення ініціює таку слідчу (розшукову) дію як огляд речей, документів та комп'ютерних даних відповідно до статті 237 КПК України «Огляд» з метою виявлення та фіксування відомостей щодо обставин вчинення кримінального правопорушення. При цьому здійснюють не тільки зовнішний його огляд як річ, а й внутрішній – змісту інформації, що міститься у цьому пристрої, як огляд комп'ютерних даних, оскільки в стільниковому радіотелефоні може міститися інформація про протиправну діяльність особи. Зважаючи на технічну особливість цього пристрою, зумовлену його роботою [5], та з метою одержання допомоги з питань, що потребують для таких дій спеціальних знань, зокрема подолання системи логічного захисту мобільного терміналу, слідчий, прокурор для участі в цьому огляді може запросити спеціаліста.

Зазвичай до зазначених дій слідчий залучає працівника оперативно-технічного підрозділу як спеціаліста у цьому напрямі згідно частини 3 статті 237 та 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 обладнення, 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 (див. Додаток № 3).

Для поглибленого розуміння відповідної слідчої (розшукової) дії, пов'язаною з технічною особливістю роботи мобільного терміналу виявленого на місці події слід розглянути поняття «огляд речей та комп'ютерних даних», що може мати значення у кримінальному судочинстві. Загалом під оглядом

речей передбачаються дії, пов’язані із зовнішнім оглядом предмета (речовин тощо) із зазначенням особливостей прикмет цього предмета, що дає можливість вирізнити його серед ідентичних. Як правило такі дії на місці події у складі СОГ здійснює інспектор-криміналіст. Щодо поняття комп'ютерних даних, то відповідно до положень базового міжнародного нормативного документа, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю (Конвенція про кіберзлочинність) комп'ютерні дані – це будь-яке надання фактів, інформації або концепцій у формі, яка є придатною для обробки у комп’ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп’ютерною системою [7]. Тобто комп’ютерні дані містять як інформацію, так і програму для виконання певних дій комп'ютерної системи. Водночас дані – це інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки, технічними та програмними засобами (статті 1 Закону України «Про електронні комунікації»). Пункт 13 статті 1 Закону України «Про електронні довірчі послуги» наводить поняття електронні дані – будь-яка інформація в електронній формі. Отже, у нашому випадку, дані – це інформація, представлена в електронному виді. У галузі криміналістики науковці поняття «комп'ютерні дані» співвідносять до поняття «комп’ютерна інформація», «цифрова інформація». Загалом комп'ютерні дані – це інформація, яка оброблюється у пристроях, системах тощо.

Працівник оперативно-технічного підрозділу на місці події у присутності понятих за допомогою апаратно-програмного комплексу «Cellebrite UFED» здійснює огляд комп’ютерних даних виявленного та вилученого з місця події слідчим стільникового радіотелефону, тобто його інформацію, не порушуючи слідів відбитків пальців рук на корпусі цього мобільного терміналу для подальшого дослідження, та створює «образ»/електронний звіт наявної інформації (див. рис. 3). Створений «образ»/електронний звіт спеціаліст записує на цифровий диск на зразок CD-R, DVD-R (носій інформації, який конструктивно та функціонально передбачений тільки для разового запису, що

у подальшому унеможливлює додаткових питань зі сторони захисту під час судового розгляду) у виді файлу, закріплює електронною міткою у виді контрольної суми (hesh symma), з використанням математичного (криптографічного) алгоритму SHA-1 (або SHA-2, MD5, CRC32) (див. рис. 4, 5). Зафіксовану інформацію на цифровому диску слід засвідчити електронним підписом особою, що здійснює ці процесуальні дії. Відповідно до рішення Верховного Суду України колегії суддів Касаційного господарського суду у справі №922/51/20 від 29 січня 2021 року електронний підпис прирівняний до власноручного підпису [3], відповідно до пункту 12 статті 1 Закону України «Про електронні довірчі послуги».

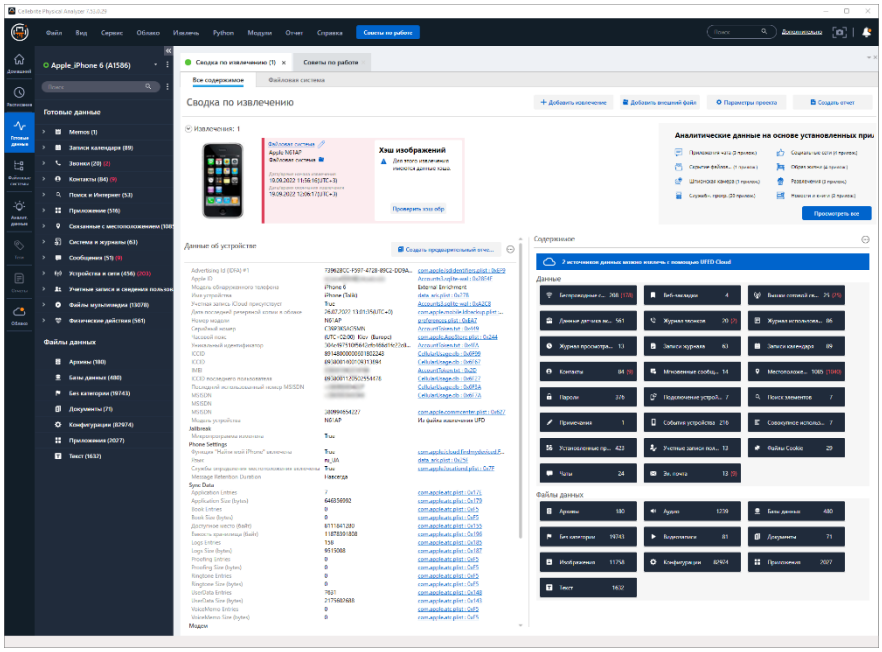

Рис. 3. Скриншот екрану апаратно-програмного комплексу «Cellebrite UFED Touch 2 Ultimate» із зображенням відкритого «образу».

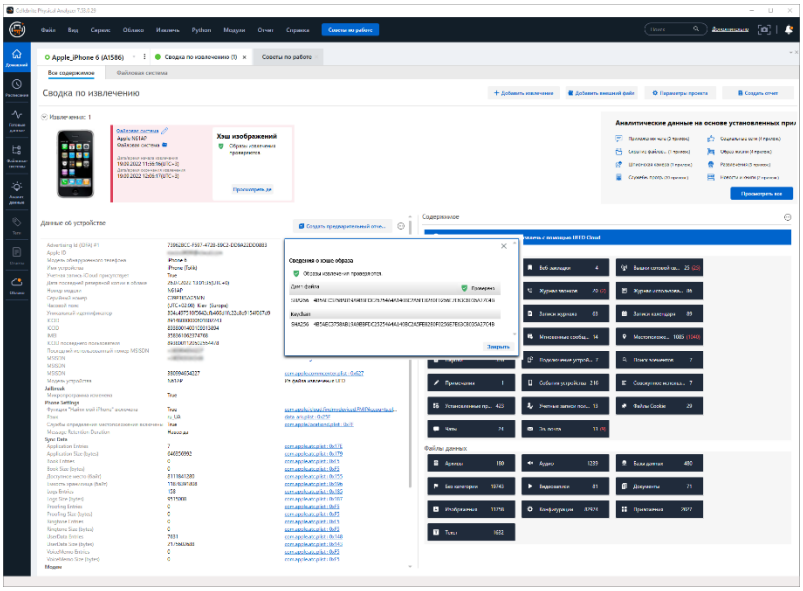

Рис. 4 Скриншот екрану апаратно-програмного комплексу «Cellebrite UFED Touch 2 Ultimate» із зображенням підрахованої хеш-суми.

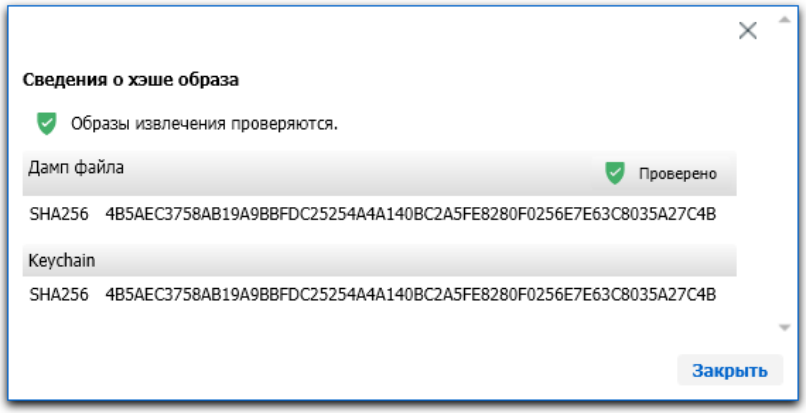

Рис. 5 Скриншот екрану апаратно-програмного комплексу «Cellebrite UFED Touch 2 Ultimate» із зображенням окремої хеш-суми «образу».

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 математичним алгоритмом хешування SHA-1 (або SHA-2, MD5, CRC32) з відомостями отриманими під час огляду інформації із 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 (див. Додаток № 3).

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).

На практиці інколи постають юридичні ситуації, коли захисник опротестовує дії слідчого щодо недопустимості доказів тобто неправомірності огляду стільникового радіотелефону без санкції слідчого судді вважаючи, що під час досудового розслідування було здійснено незаконний (без постанови слідчого судді) доступ до відомостей з електронних інформаційних систем, який оформлено як протокол огляду предмета – телефона.

Відповідно до рішення Верховного Суду України колегії суддів Касаційного кримінального суду у справі № 727/6578/17 від 15 квітня 2020 року зняття інформації з електронних інформаційних систем або їх частин можливе без дозволу слідчого судді, якщо доступ до них не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Тому Верховний Суд України на вбачає жодних порушень вимог кримінального процесуального закону при дослідженні інформації, яка була наявна в мобільному телефоні шляхом увімкнення телефону та огляду текстових повідомлень, які в ньому знаходились *(листування в телеграм-каналі)* та доступ до яких не був пов`язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем. За таких обставин Верховний Суд України на вбачає жодних порушень вимог кримінального процесуального закону під час огляду цього кримінального провадження [2].

Коментуючи рішення Верховного Суду України колегії суддів Касаційного кримінального суду розглянемо поняття мобільного телефону, а

саме стільникового радіотелефону як мобільний термінал. Відповідно до пункту 59 статті 1 Закону України «Про електронні комунікації» (далі – Закон) мобільний зв'язок – електронні комунікації із застосуванням радіотехнологій, під час яких кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення електронної комунікаційної мережі. Разом із тим згідно пункту 41 статті 1 цього Закону кінцеве (термінальне) обладнання – обладнання, призначене для з'єднання з кінцевим пунктом електронної комунікаційної мережі з метою забезпечення доступу до електронних комунікаційних послуг. Де електронна комунікаційна послуга – послуга, що полягає в прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг (пункт 27 статті 1 Закону). Зважаючи на зазначене стільниковий радіотелефон як мобільний термінал становить кінцевий елемент електронної комунікаційної мережі, зокрема мобільного зв'язку. Тому стільниковий радіотелефон до електронних інформаційних систем не належить.

Якщо особа затримана за підозрою у вчиненні кримінального правопорушення добровільно надала оперативним працівникам (слідчим) доступ до інформації (комп'ютерних даних) свого стільникового радіотелефону, то у такому випадку застосування апаратно-програмного комплексу «Cellebrite UFED» не обов'язковий, оскільки одна із основних функцій цього комплексу це подолання системи логічного захисту мобільних терміналів. Однак у цій ситуації слід у протоколі з огляду предмета зазначити про добровільність наданої їм такої можливості.

У межах 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 також залучають спеціаліста для огляду мобільного терміналу (стільникового

радіотелефону) та SIM-картки безпосередньо на місці обшуку з подальшим його оглядом.

Для здійснення відповідної процесуальної дії слідчий залучає працівника оперативно-технічного підрозділу як спеціаліста згідно частини 1 статті 236 та статті 71 КПК України. У такому разі слідчий виносить відповідну постанову згідно частини 3 статті 110 КПК України, а до оперативно-технічного підрозділу надсилається відповідний лист про необхідність проведення обшуку та, якщо буде виявлений стільниковий радіотелефон, його огляду працівником оперативно-технічного підрозділу, у якому зазначається дата та місце проведення огляду (без зазначення прізвища) (див. Додаток № 1, № 2).

Слідчий, прокурор під час проведення обшуку має право відкривати закриті приміщення, сховища, речі, долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх відкрити чи зняти (деактивувати) систему логічного захисту (частина 6 статті 236 КПК України).

Якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку (частина 6 статті 236 КПК України).

Слід зазначити, що особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку.

При обшуку слідчий, прокурор має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення обшуканого житла чи іншого володіння особи чи окремих

речей, виготовляти відбитки та зліпки, оглядати і вилучати документи, тимчасово вилучати речі, які мають значення для кримінального провадження. Предмети, які вилучені законом з обігу, підлягають вилученню незалежно від їх відношення до кримінального провадження. Вилучені речі та документи, які не входять до переліку, щодо якого прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку, та не відносяться до предметів, які вилучені законом з обігу, вважаються тимчасово вилученим майном (частина 7 статті 236 КПК України).

Обшук житла чи іншого володіння особи на підставі ухвали слідчого судді в обов'язковому порядку фіксується за допомогою аудіо- та відеозапису (частина 10 статті 236 КПК України).

У разі виявлення стільникового радіотелефону та/або SIM-картки під час обшуку приміщення порядок застосування апаратно-програмного комплексу «Cellebrite UFED», вилучення інформації із мобільного терміналу та подальша процедура її документування аналогічна процесуальній дії з огляду.

За потреби слідчий направляє цифровий носій із створеним «образом»/електронним звітом вилученого стільникового радіотелефону до оперативно-технічного підрозділу для здійснення аналізу вилученої інформації із створеного «образу».

4. Порядок документування заходу із зняття інформації з електронних інформаційних систем (мереж)

На практиці під час виявлення, припинення та розслідування кримінальних правопорушень інколи постає нагальна потреба у здійсненні заходів, пов’язаних із втручанням у приватне спілкування шляхом отримання інформації з електронних інформаційних систем (мереж) без (або з) відома її власника, володільця або утримувача. Такі дії позначаються як зняття інформації з електронних інформаційних систем (мереж) та здійснюються у межах відкриття кримінального провадження або заведення оперативно-розшукової справи. Зняття інформації з електронних інформаційних систем (мереж) у межах кримінального провадження під час досудового розслідування відноситься до різновиду негласних слідчих (розшукових) дій та регламентується Кримінальним процесуальним кодексом України, у межах оперативно-розшукової справи – до різновиду оперативно-технічного заходу та регламентується Законом України «Про оперативно-розшукову діяльність» і відомчими нормативно-правовими актами.

У зв’язку з цим у правозастосовній діяльності працівники правоохоронних органів здійснюють заходи із зняття інформації з електронних інформаційних систем (мереж) у двох напрямах: оперативно-розшуковому та кримінальному процесуальному.

Розглянемо ці напрями докладніше.

У оперативно-розшуковому напрямі захід із зняття інформації з електронних інформаційних мереж здійснюється у межах оперативно-розшукової справи, заведеної за наявності підстав, визначених частиною першою статті 6 Закону України «Про оперативно-розшукову діяльність» за тяжкими або особливо тяжкими злочинами відповідно до пункту 9 частини 1 статті 8 та частини 2 статті 8 Закону України «Про оперативно-розшукову діяльність».

У кримінальному процесуальному напряму дії із зняття інформації з електронних інформаційних систем здійснюються у межах кримінального

провадження відповідно до статті 264 КПК України у виді негласної слідчої (розшукової) дії, а саме

«1. Пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування.

2. 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.

3. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування» [9].

Розглянемо наведені частини статті 264 КПК України детальніше.

Частина 1 цієї статті забезпечує нормативно-правову регламентацію втручання у приватне спілкування шляхом зняття інформації з електронних інформаційних систем. Сутність відповідної негласної слідчої (розшукової) дії полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частин, без відома власника, володільця або утримувача системи. Зазначена негласна слідча (розшукова) дія проводиться, у разі якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування.

Для найкращого розуміння поняття «зняття інформації з електронних інформаційних систем» розглянемо тлумачення терміну системи та її види. Відповідно до тлумачного енциклопедичного словника сучасної української

мови система (від дав.-гр. σύστημα - «сполучення», «ціле», «з'єднання») це:

4) Сукупність яких-небудь елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням;

6) Будова, структура, що становить єдність закономірно розташованих та функціонуючих частин. // Технічний комплекс, що складається із взаємопов'язаних споруд, механізмів, машин і т. ін. // Марка, тип, конструкція яких-небудь машин, їх частин і т. ін. *Система парашута*. // Сукупність предметів, пристроїв і т. ін. однакового призначення [1, с. 1126].

Законодавець статтею 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» наводить деякі види систем, зокрема інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів; інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле; електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [14].

Враховуючи наведене під електронною інформаційною системою розуміється взаємозв’язок технічних засобів (комп’ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп’ютерних мереж та/або інших технічних засобів) з інформаційними технологіями, що реалізують інформаційні процеси та призначені для збору, зберігання, обробки, пошуку, розповсюдження, передачі та надання впорядкованої інформації (даних) в електронному виді.

Закон України від 31.05.2005 р. «Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» наводить інші поняття, що передбачено частиною 1 статті 264 КПК України, а саме: володілець інформації – фізична або юридична особа, якій належать права на інформацію; власник інформації (системи) у такому випадку вважається – фізична або

юридична особа, якій належить право власності на інформацію (систему). Утримувач – фізична чи юридична особа, яка постійно або тимчасово володіє, застосовує та несе відповідальність за використання предмета утримання.

Підставами для проведення зняття інформації з електронних інформаційних систем є відомості, що в електронній інформаційній системі або її частині є інформація, що має значення для досудового розслідування.

Частина 1 статті 264 КПК України також визначає, що відомості можуть міститися як в електронній інформаційній системі, так і в її частинах. Під частинами електронних інформаційних систем слід вважати бази даних, системи управління базами даних, клієнтське програмне забезпечення, доступ до яких обмежується їх власником, володільцем або утримувачем, зокрема застосуванням системи логічного захисту.

Об'єктами зняття інформації з електронних інформаційних систем, відповідно до пункту 1.11.6 наказу ГПУ, МВС, СБУ, АДПС, МФ, МЮ України від 16.11.2012 № 114/1042/516/1199/936/1687/5 «Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні», є електронно-обчислювальні машини (комп’ютери), автоматизовані системи, комп’ютерні мережі, мережі електрозв’язку, які накопичують, обробляють, зберігають або передають відомості про тяжкі та особливо тяжкі злочини.

При цьому термін мережа, згідно тлумачного енциклопедичного словника, розглядається як сукупність яких-небудь шляхів, ліній зв’язку, каналів і т.ін., розташованих на певній території [1, с. 519]; комп’ютер – електронна обчислювальна машина [1, с. 446]; комп’ютерна мережа – сукупність комп’ютерів, зв’язаних каналами передачі інформації, та необхідного програмного забезпечення і технічних засобів, призначених для організації розподіленої обробки інформації [1, с. 446].

Проведення негласної слідчої (розшукової) дії, регламентованої статтею 264 КПК України забезпечується зняттям інформації, що обробляється, зберігається на персональному комп'ютері, або декількох персональних

комп'ютерах, об'єднаних у локальну мережу, або ж зовнішніх накопичувачах інформації, що приєднувалися до електронних інформаційних систем. Проведення цієї слідчої (розшукової) дії відбувається негласно, у порядку, встановленому статтями 246, 248, 250 КПК України. Слідчий суддя може дати дозвіл на проведення відповідних дій щодо зняття інформації з електронних інформаційних систем або її частин у випадках, якщо ПЕОМ, декілька ПЕОМ, об'єднаних у локальну мережу, зовнішні накопичувачі електронної інформації належать, належали або ж використовувались підозрюваним, обвинуваченим у вчиненні злочину, за наявності обґрунтованих підстав уважати, що в них зберігалася або оброблялася інформація, яка має значення для виявлення, припинення та розслідування тяжкого або особливо тяжкого злочину, щодо якого у встановленому законом порядку ведеться кримінальне провадження.

Зняття інформації з електронних інформаційних систем або їх частин може здійснюватися як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного проникнення. Негласне зняття інформації із засобів електронно-обчислювальної техніки (комп’ютера) полягає у застосуванні спеціальних технічних засобів із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диску (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого, що можуть містити інформацію, яка має значення у кримінальному провадженні. Програмне проникнення до електронних інформаційних систем (їх частин) здійснюється шляхом застосування спеціальних програмних продуктів, які забезпечують копіювання інформації, що обробляється на ПЕОМ підозрюваного, обвинуваченого, на віддалений комп'ютер, що перебувають у користуванні уповноваженого органу, що проводить цю негласну слідчу (розшукову) дію.

Відповідно до частини 2 статті 264 КПК України 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. Уповноваженими органами в процесі збору і фіксації інформації, що має значення для кримінального провадження, може проводитись цілеспрямований пошук серед комп'ютерних систем та мереж відкритої інформації, у тому числі всесвітньої мережі Інтернет, з метою виявлення необхідних у справі відомостей. Серед великих масивів інформації, що локалізуються в соціальних мережах Інтернету, може бути отримана інформація щодо окремих осіб, які підозрюються в підготовці та вчиненні злочинів, їх зав’язків, та багато інших відомостей, що можуть сприяти вирішенню завдань досудового розслідування. Оскільки ця інформація є загальнодоступною, дозволу слідчого судді на її пошук та фіксацію кримінальний процесуальний закон не потребує, через те, що не відбувається обмеження приватності спілкування окремих осіб.

Рішення про проведення зняття інформації з електронних інформаційних систем (мереж) приймає слідчий, прокурор, а також слідчий суддя апеляційного суду за клопотання прокурора, або за клопотанням слідчого (у межах ОРС – оперативного працівника), погодженого з прокурором, згідно частини 3 статті 246 КПК України (див. Додаток № 4). Прокурор має право заборонити проведення або припинити подальше проведення негласної слідчої (розшукової) дії або оперативно-розшукового заходу.

Відповідно у клопотанні до суду, що вноситься слідчим, прокурором (у межах ОРС – оперативним працівником) повинні бути вказані крім загальних даних відомості, що стосуються зняття інформації з електронних інформаційних систем (мереж), зокрема серійні номери ПЕОМ, зовнішніх накопичувачів інформації, з яких відбуватиметься зняття інформації із використанням спеціальних технічних засобів та спеціального програмного забезпечення, що забезпечують безпосереднє фізичне або програмне проникнення до інформаційної системи або її частини тощо.

В ухвалі для проведення зняття інформації з електронних інформаційних систем (мереж) зазначається:

орган, який звернувся з клопотанням;

дата заведення кримінального провадження (оперативно-розшукової справи) щодо особи;

дані про Єдиний реєстр досудових розслідувань;

дані про особу;

стаття Кримінального кодексу України, якою передбачено кримінальну відповідальність за діяння, вчинене особою, чи до якого вона готується;

ідентифікаційні ознаки електронної інформаційної системи (найменування електронної інформаційної системи, фізична адреса розташування її файлових серверів та робочих станцій або електронна адреса в мережі Інтернет, її власник, володілець або утримувач) та спосіб, яким обмежений доступ до неї;

підстави надання дозволу (з посиланнями на них);

назва відповідної негласної слідчої (розшукової) дії (оперативно-технічного заходу);

строк дії ухвали, який не може перевищувати двох місяців (вказаний строк може бути продовженим) (див. Додаток № 5).

Клопотання та ухвала суду про надання дозволу на здійснення заходу реєструються в апарату суду без розкриття відомостей про особу та змісту заходу, який передбачається здійснити.

Два примірники ухвали суду (у разі його здійснення стосовно кількох осіб – щодо кожної особи) передаються уповноваженому представникові підрозділу. Один примірник додається до справи (провадження), а інший – видається підрозділу, працівники якого залучаються до здійснення заходу. Якщо суд відмовив у видачі дозволу, один примірник ухвали суду видається уповноваженому представникові підрозділу.

Отримавши ухвалу слідчого судді про дозвіл на зняття інформації з електронної інформаційної системи слідчий у письмовій формі, у порядку пункту 2 частини 2 статті 40, статті 41, частини 6 статті 246 КПК України, дає доручення оперативному підрозділу, що здійснює такі дії на проведення цієї негласної слідчої (розшукової) дії. Ці дії, але в межах оперативно-розшукового заходу оперативний працівник за матеріалами ОРС, отримавши ухвалу слідчого

суді письмово, у порядку частини 2 статті 8 Закону України «Про оперативно-розшукову діяльність», оформлює завдання оперативному підрозділу, що здійснює такий оперативно-технічний захід. У разі застосування апаратно-програмного комплексу «Cellebrite UFED» для отримання інформації з стільникового радіотелефону у дорученні на проведення НСРД (завданні – на проведення ОТЗ), крім зазначених у бланку відомостей, обов'язково вказується ідентифікатор IMEI стільникового радіотелефону та/чи абонентський номер. До доручення (завдання) додається примірник ухвали слідчого судді апеляційного суду або постанова керівника підрозділу-ініціатора (у разі невідкладності) та матеріальний носій інформації.

Уповноважені працівники оперативно-технічних підрозділів у ході проведення відповідної негласної слідчої (розшукової) дії (оперативно-технічного заходу) відбирають ту інформацію, яка має значення у кримінальному провадженні (оперативно-розшуковій справі), фіксують її на матеріальних носіях, що можуть забезпечити подальше відтворення цієї інформації. Проте залежно від виду мобільного терміналу та поставлених для цього заходу завдань оперативно-технічний підрозділ вирішує, який тип технічного засобу та вид програмного забезпечення застосовувати. Для отримання інформації з стільникового радіотелефону (SIM-картки) зазвичай виконавець застосовує апаратно-програмний комплекс «Cellebrite UFED». У результаті його застосування виконавець створює «образ»/електронний звіт наявної інформації мобільного терміналу, записує його на матеріальний носій на зразок CD-R, DVD-R у виді файлу, закріплює електронною міткою у виді контрольної суми (hesh symma), з використанням математичного алгоритму SHA-1 (SHA-2 або MD5). У подальшому мобільний термінал та матеріальний носій повертають листом до підрозділу-ініціатора (див. Додаток № 6, № 7).

Отримавши матеріальний носій слідчий (оперативний працівник) вивчає інформацію, складає протокол із дотриманням вимог статті 104-107, 252 та 265 КПК України. Додатками до протоколу про зняття інформації з електронних інформаційних систем (мереж) можуть бути матеріальні носії

інформації, отримані за результатами проведення відповідної негласної слідчої (розшукової) дії (оперативно-технічного заходу). У протоколі також слід вказати на технічні засоби, вид програмного забезпечення, яке використовувалось для фіксації та відтворення отриманої за результатами негласних слідчих (розшукових) дій (оперативно-технічного заходу) інформації, з метою забезпечення можливості ознайомлення із цією інформацією на подальших стадіях кримінального провадження.

У протоколі зазвичай зазначаються дата його складання, посада, прізвище та ініціали особи, у провадженні якої перебуває справа, номер справи, за якою проводився захід, номер ухвали слідчого судді, дата її винесення та найменування суду, вид заходу та строки його проведення, найменування підрозділу, працівники якого залучалися до проведення заходу, дані про особу, стосовно якої проводився захід, результати проведення заходу (наявність або відсутність фактичних даних про можливі протиправні діяння особи, відповідальність за які передбачена КК України), відомості про матеріальні носії інформації (носії комп'ютерних даних та інші матеріали, які пояснюють зміст протоколу) та місце їх зберігання.

Забороняється зазначати в протоколі та зберігати в будь-якому іншому вигляді відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій.

Протягом 24 годин після припинення зняття інформації з електронних інформаційних систем (мереж) відповідно до частини 3 статті 252 КПК України уповноважена посадова особа оперативного підрозділу передає протокол прокурору для прийняття ним рішення про використання як доказ інформації, отриманої внаслідок застосування цих форм втручання у приватне спілкування, у цілому або певного її фрагмента.

Відомості, речі та документи, отримані в результаті проведення негласної слідчої (розшукової) дії (оперативно-технічного заходу), які прокурор не визнає необхідними для подальшого проведення досудового розслідування, повинні бути негайно знищені на підставі його рішення, викладеного в постанові

(частина 1 статті 255 КПК України). Інформація, отримана в результаті проведення негласних слідчих (розшукових) дій (оперативно-технічного заходу) до постановлення ухвали слідчого судді, якщо він постановив ухвалу про відмову в наданні дозволу на проведення негласної слідчої (розшукової) дії (оперативно-технічного заходу), повинна бути знищена (частина 3 статті 250 КПК України).

Слід зазначити, що відповідно до частини 2 статті 99 КПК України «Матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України "Про оперативно-розшукову діяльність", за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази».

Особа, конституційні права якої були тимчасово обмежені під час проведення негласних слідчих (розшукових) дій, а також підозрюваний, його захисник мають бути письмово повідомлені прокурором або за його дорученням слідчим про таке обмеження. Відповідне повідомлення про факт і результати негласної слідчої (розшукової) дії повинно бути здійснене протягом дванадцяти місяців з дня припинення таких дій, але не пізніше звернення до суду з обвинувальним актом (стаття 253 КПК України).

Додаток № 1

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ *(назва)*
Управління (назва)
вул. *(назва)*, 00, м. *(назва)*, 00000,
тел. (000) 000-00-00, (000) 000-00-00
_*@**.**.**
ЄДРПОУ: 00000000

00.00.0000 № 0000/00/000/00-0000

Начальникові *(назва служби)*
Національної поліції України
(спеціальне звання)
(ім'я та прізвище)

Про виділення спеціаліста

Шановний пане (ім'я)!

Управлінням *(назва)* Департаменту *(назва)* Національної поліції України, здійснюється оперативне супроводження кримінального провадження №00000000000000000 від 00.00.0000 року, за ознаками кримінального правопорушення, передбаченого ч. 0 ст. 000 КК України.

У ході досудового розслідування планується проведення обшуку відповідно до ухвали слідчого судді *(суд)* 0-**-000/00, 0-**-000/00, 0-**-000/00 від 00.00.0000 року.

З метою забезпечення швидкого, повного та ефективного досудового розслідування, встановлення фактичних даних, які вказують на наявність, або відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню, керуючись ст. 40, ст. 71, ч. 1 ст. 236 КПК України прошу виділити 00.00.0000 працівника (-ів) ДОТЗ НП України з використанням програмно-апаратного комплексу «Cellebrite UFED Touch 2 Ultimate» у проведенні відповідної слідчої (розшукової) дії.

З повагою

(посада)
(спеціальне звання) **(ім'я та прізвище)**

Додаток № 2

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ *(назва)*
Управління (назва)
вул. *(назва)*, 00, м. *(назва)*, 00000,

00.00.0000 № 00-**/000/00-0000

Начальникові *(назва служби)*
Національної поліції України
(спеціальне звання)
(ім'я та прізвище)

Про надання інформації

Шановний пане (ім'я)!

У провадженні слідчого відділу *(назва)* управління *(назва)* Національної поліції у м. *(назва)* перебуває кримінальне провадження №00000000000000000, дані щодо якого внесено до Єдиного реєстру досудових розслідувань 00.00.0000 року, за ознаками кримінального правопорушення, передбаченого ч.0, ст. 000 КК України.

Проведенням досудового розслідування по зазначеному кримінальному провадженню встановлено, що на території *(назва)* району у м. *(назва)*, та інших містах України групою осіб, *(фактичні дані про протиправні діяння)*.

У ході проведення досудового розслідування під час обшуків, що проводились 00.00.0000, було виявлено та вилучено низка мобільних терміналів (стільникових радіотелефонів) та комп'ютерної техніки.

З метою забезпечення ефективного та повного розслідування, а також дослідження у подальшому отриманої інформації на предмет наявності чи відсутності в ній фактів та обставин, що мають значення для кримінального провадження, просимо Вас виділити співробітника з метою залучення як спеціаліста для допомоги в проведенні огляду відповідних мобільних терміналів.

Додаток: стільниковий радіотелефон *(марка, модель)*, IMEI – 000000000000000, з сім-картою мобільного оператора (назва) з абонентським номером +380000000000, ноутбук (марка, модель), серійний номер *000*00*-0000-00*0-00**-*00000***000 та блок живлення.

З повагою

(посада)
(спеціальне звання) **(ім'я та прізвище)**

Додаток № 3

ПРОТОКОЛ
огляду предмета

Місто (сел.) _Дніпро__ «20» 11.2022 року

Огляд почато о “20” год. “40” хв.
Огляд закінчено о “22” год. “50” хв.

Слідчий СВ Індустріального ВП Дніпровського ВП ГУ НП у Дніпропетровській області капітан поліції Іванов І.І. _____
(слідчий, найменування органу, прізвище, ім’я, по батькові)
на підставі _кримінального провадження № 12012160_____
відповідно до ст.ст. 104, 105, 106, 223, 237 КПК України:
у присутності понятих:
1) _Козіна Альберта Федоровича, 28.02.1965 р. н., який мешкає у м. Дніпро, вул. Косіора, 71, кв. 15;_____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
2) _Буніна Валерія Миколайовича, 21.01.1983 р. н., який мешкає у м. Дніпро, вул. Косіора, 71, кв. 4,_____
(прізвище, ім’я, по батькові, дата народження, місце проживання)
яким відповідно до ст. 11, 13, 15, 223 КПК України роз’яснено їхні права і обов’язки.

1) _____ 2) _____
(підпис) (підпис)

За участю потерпілого:
Сомова Сергія Семеновича, 14.02.1975 р. н., який мешкає у м. Дніпро, вул. Косіора, 71, кв. 10_____,
(прізвище, ім’я, по батькові, дата народження, місце проживання)
якому відповідно до ч. 1, 2 ст. 56, ст. 57 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю спеціаліста:
інспектора-криміналіста НДЕКЦ у Дніпропетровській області лейтенанта поліції Котова Сергія Івановича_____,
(прізвище, ім’я, по батькові, місце роботи)
якому відповідно до ч.4,5 ст.71 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю спеціаліста:
оперуповноваженого УДОТЗ НП у Дніпропетровській області капітана поліції Сергієва Івана Івановича_____,
(прізвище, ім’я, по батькові, місце роботи)
якому відповідно до ч.4,5 ст.71 КПК України роз’яснено його права і обов’язки.

_____
(підпис)

За участю власника (користувача) приміщення чи іншого володіння особи
Сомова Сергія Семеновича, який мешкає у м. Дніпро, вул. Косіора, 71, кв. 10
(прізвище ім'я, по батькові, адреса)

_____
(підпис)

у квартирі за адресою: м. Дніпро, вул. Косіора, 71, кв. 10 провів огляд виявленого стільникового радіотелефону «Samsung A 30» із заводським номером (IMEI) 1234567891234._____

Перед початком огляду предмета зазначеним особам роз'яснено їхнє право бути присутніми при всіх діях, які проводяться в процесі огляду, робити зауваження, що підлягають занесенню до протоколу. Особам, які беруть участь у проведенні огляду, також роз'яснено вимоги ч. 3 ст. 66 КПК України про їх обов'язок не розголошувати відомості щодо проведеної процесуальної дії, а також про застосування технічних засобів фіксації, умови та порядок їх використання.

Під час огляду застосовано технічні засоби: цифровий фотоапарат "Nikon"__
(вказується застосування фото-, відеозйомки, інших технічних та спеціальних засобів, їх найменування, технічні параметри)

Проведеним оглядом встановлено: об'єктом огляду є стільниковий радіотелефон «Samsung A 30» з заводським номером (IMEI) 1234567891234 сірого кольору прямокутної плоскої форми_____

Під час огляду виявлено: на верхньому боці телефону в його правій частині є подряпина у формі коми довжиною 3 міліметри. Під кришкою на задній панелі телефону міститься заводський номер (IMEI) 1234567891234_____

Виявлено під час огляду та вилучено: оглянутий стільниковий радіотелефон «Samsung A 30» поміщений у поліетиленовий пакет чорного кольору, горловина якого зав'язана капроновою ниткою білого кольору. На вузол зав'язаної нитки наклеєна паперова бирка. На бирці зазначено «20 вересня 2021 року Індустріальний ВП Дніпровського ВП ГУ НП у Дніпропетровській області, стільниковий радіотелефон «Samsung A 30» з заводським номером (IMEI) 1234567891234._____

поняті:
1) Козін А.Ф. /підпис/;
2) Бунін В.М. /підпис/;
спеціаліст Котов С.І. /підпис/;
спеціаліст Сергієв І.І. /підпис/;
слідчий Іванов І.І. /підпис/

Під час огляду застосовано технічні засоби: фотоапаратом "Nikon" зроблені два фотознімки: (№ 1 – фіксація зовнішнього вигляду телефона з подряпиною

на верхньому боці телефону в його правій частині; № 2 – фіксація вигляду задньої панелі телефону з його заводським номером (IMEI). Програмно-апаратним комплексом «Cellebrite UFED Touch 2 Ultimate» отримані комп'ютерні дані з стільникового радіотелефону «Samsung A 30».
(вказується застосовування фото-, відеозйомки, інших технічних та спеціальних засобів, їх технічні параметри)

Огляд проводився в квартирі за адресою: м. Дніпро, вул. Косіора, 71, кв. 10 при штучному освітленні
(вказуються погодні умови, освітлення, температура повітря, інші необхідні дані)

До протоколу огляду додаються: фотознімки з фотоапарату "Nikon", стільниковий радіотелефон «Samsung A 30» із заводським номером (IMEI) 1234567891234, цифровий диск CD-R з контрольною сумою, з використанням.
(план (схематичний чи масштабний); схема місцевості; схема огляду місця події; схема доріжки слідів; схема сліду низу взуття; схема сліду знаряддя зламу; інше)
алгоритму SHA-1.
(носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу)

Протокол прочитано, записано слідчим зачитаний вголос, записано в точній відповідності до проведених процесуальних дій та отриманих результатів. Зауважень від учасників не надійшло.
(зауваження учасників огляду)

З протоколом ознайомлені:

учасники:

1. Котов С.І. /_____/
(прізвище, ім'я, по батькові) (підпис)
2. Сергієв І.І. /_____/
(прізвище, ім'я, по батькові) (підпис)
3. Сомов С.С. /_____/
(прізвище, ім'я, по батькові) (підпис)

поняті:

1. Козін А.Ф. /_____/
(прізвище, ім'я, по батькові) (підпис)
2. Бунін В.М. /_____/
(прізвище, ім'я, по батькові) (підпис)

Огляд провів та протокол склав:
слідчий СВ Індустріального ВП Дніпровського ВП
ГУ НП України в Дніпропетровській області
капітан поліції _____ **І.І. Іванов**
(підпис)

Додаток № 4

КЛОПОТАННЯ
про дозвіл на проведення негласної слідчої (розшукової) дії

Місто (сел.) _____ «_____» _____ 20__року

_____,
(слідчий, посада, найменування органу, ініціали, прізвище)
розглянувши матеріали досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № _____ від «____» _____20 __ р., за ознаками _____, –
(правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) Закону України про кримінальну відповідальність)

ВСТАНОВИВ:

_____
(короткий виклад обставин злочину, у зв'язку з розслідуванням якого подається клопотання;
_____
правова кваліфікація злочину із зазначенням статті (частини статті) КК України;
_____
відомості про особу (осіб), місце або річ, щодо яких необхідно провести негласну слідчу (розшукову) дію;
_____
вид негласної слідчої (розшукової) дії та обґрунтування строку її проведення;
_____
обставини, що дають підстави підозрювати особу у вчиненні злочину;
_____
обґрунтування неможливості отримання відомостей про злочин та особу, яка його вчинила, в іншій спосіб;
_____
відомості залежно від виду негласної слідчої дії про ідентифікаційні ознаки, які дозволять унікально
_____
ідентифікувати абонента спостереження, електронно комунікаційну мережу, кінцеве обладнання тощо;
_____
обґрунтування можливості отримання під час проведення негласної слідчої (розшукової) дії доказів,
_____
які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування
_____
обставин злочину або встановлення осіб, які його вчинили)

Враховуючи викладене, керуючись вимогами ст. 40, 246, 248 КПК України, –

ПРОШУ:

Надати дозвіл на проведення
_____.
(вид негласної слідчої (розшукової) дії та строк її проведення)

Додаток: Витяг з Єдиного реєстру досудових розслідувань за № _____
від «___» _____ 20 __ р.

Слідчий _____
(посада, найменування органу, підпис, прізвище, ініціали)

«ПОГОДЖЕНО»

Прокурор _____
(посада, найменування органу, підпис, прізвище, ініціали)

«___» _____ 20 ___ року

Додаток № 5

УХВАЛА

ІМЕНЕМ УКРАЇНИ

УХВАЛИВ:

Клопотання слідчого _____ Національної поліції у м. _____ (ПІБ)., у кримінальному провадженні № 00000000000000000, відомості якого внесено до Єдиного реєстру досудових розслідувань 00.00.0000 року, за ознаками кримінального правопорушення, передбаченого ч. 0 ст. 000 КК України, погоджено _____ прокуратури м. _____ (ПІБ) – задовольнити.

Надати слідчому _____ Національної поліції у м. _____ (ПІБ)., дозвіл на проведення негласних слідчих (розшукових) дій, що тимчасово обмежують права та свободи людини, а саме – зняття інформації з електронних інформаційних систем, що полягає в пошуку, виявленні і фіксації відомостей, що містяться в електронній інформаційній системі або її частині, доступ до електронної інформаційної системи або її частини, а також отриманні таких відомостей без відома її власника, пов'язаного із подоланням систем логічного захисту, а саме текстових, аудіо, відео повідомлень, документів та файлів, використовуючи месенджери «Viber», «WhatsApp», «Telegram», «Signal» та інші, зареєстровані за мобільним терміналом IMEI: 0000000000000000 з абонентським номером +380000000000, якими у своїй протиправній діяльності користується гр. (ПІБ), 00.00.0000 року народження, оскільки в інший спосіб, крім проведення негласної слідчої (розшукової) дії, отримати таку інформацію не можливо.

Зазначені заходи провести строком 60 діб з моменту підписання ухвали.

Ухвала оскарженню не підлягає.

Додаток № 6

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

Департамент оперативно-технічних заходів

вул. Богомольця, 10, м. Київ, 01601,
тел. (044) 271-69-87, (044) 271-63-66
e-mail: ****@******.***.**

Начальникові *(назва служби)*
Національної поліції України
(спеціальне звання)
(ім'я та прізвище)

0000 року № _____
На №00**/000/00-0000 від 00.00.0000

Про повернення матеріалів

Повертаємо після опрацювання технічні засоби у межах кримінального провадження від 00.00.0000 № 00000000000000000 за ознаками кримінального правопорушення, передбаченого ч. 0 ст. 000 КК України.

Додаток (лише адресатові):

1. стільниковий радіотелефон *(марка, модель)*, IMEI – 000000000000000, з сім-карткою мобільного оператора (назва) з абонентським номером +380000000000;
2. ноутбук (марка, модель), серійний номер *000*00*-0000-00*0-00**-*00000***000 та блок живлення.

З повагою

(посада)
(спеціальне звання) **(ім'я та прізвище)**

Додаток № 7

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

Департамент оперативно-технічних заходів

вул. Богомольця, 10, м. Київ, 01601,
тел. (044) 271-69-87, (044) 271-63-66
e-mail: dotz@police.gov.ua

Начальникові *(назва служби)*
Національної поліції України
(спеціальне звання)
(ім'я та прізвище)

_____ року № _____
На № 0000т/00/00 - 0000 від 00.00.0000

Про повернення носіїв

Шановний пане (ім'я)!

Повертаємо надіслані носії після запису інформації, отриманої в результаті проведення НСРД № 8, у межах кримінального провадження від 00.00.0000 № 00000000000000000 відповідно до ухвали слідчого судді *(суд)* № 00-00/000/0000/0000 та № 00-00/000/0000/0000.

Повідомляємо, що з метою перевірки цілісності даних на носії розраховується контрольна сума, з використанням алгоритму SHA-1.

Додаток (лише адресату):

1. Картка пам'яті Micro SD інв. № 000т від 00.00.0000, таємно, розмір – 00 000 000 000 байт, SHA-1: *000*00*00*0*00*00**000*000000*000*0**00-0000000*;
2. Картка пам'яті Micro SD інв. № 000т від 00.00.0000, таємно, розмір – 0 000 000 000 байт, SHA-1: 00000000**0*0*00000*00***0000*000**0*00*-0000000*.

З повагою

(посада)
(спеціальне звання) **(ім'я та прізвище)**

Список використаних джерел

1. Великий тлумачний словник сучасної української мови. Київ; Ірпінь: ВТФ "Перкун", 2002. 1440 с.

2. Верховний Суд. Касаційний кримінальний суд (2020, квітень 4.). *Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші злочини проти здоров'я населення* : постанова у справі № 727/6578/17 провадження № 51-4494 км 19.

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

4. Говоруха В.І., Степанов В.А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. *Інформація і право*. № 3 (34)/2020. С. 69-74.

5. Засоби і системи зв'язку ОВС : навчальний посібник / М.В. Кобець, Е.В. Ланевський, О.В. Яковенко. Київ : Нац. ак. вн. справ України, 2004. 83 с.

6. 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. ак. внут. справ. 2023. С. 70-73.

7. Кобець М.В. Дії слідчого під час виявлення на місці події мобільних терміналів (стільникових радіотелефонів). *Криміналістичний вісник* : науково-практичне видання. Київ : Держ. наук.-дослід. експерт.-кримінал. центр МВС України, 2023. № 1 (39).

8. Кобець М.В. Процедура застосування сучасних програмно-технічних засобів зняття інформації з електронних інформаційних систем. *Актуальні питання виявлення та розкриття злочинів Національної поліції: вітчизняний та зарубіжний досвід* : матер. міжнарод. наук.-практ. круглого столу. (м. Київ, 19 лют. 2020 р.). Київ : Нац. ак. вн. справ, 2020. С. 89-92.

9. Конвенція Ради Європи про кіберзлочинність від 23.11.2001, ратифіковано із застереженнями і заявами Законом № 2824-IV від 07.09.2005.

ВВР, 2006. № 5-6. ст. 71.

10. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI.

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

12. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX.

13. 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.

14. 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.

15. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України (ВВР), 1994. № 31. ст. 286.

16. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. // Відомості Верховної Ради, 1992. № 22. Ст. 303.

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