УДК 343.982: 343.137.5 DOI: 10.37025/1992-4437/2023-39-1-52

М. В. Кобець,
кандидат юридичних наук, старший науковий співробітник,
доцент кафедри оперативно-розшукової діяльності,
Національна академія внутрішніх справ, м. Київ
ORCID: https://orcid.org/0000-0002-2233-0946
email: mv.kobets@ukr.net

ДІЇ СЛІДЧОГО ПІД ЧАС ВИЯВЛЕННЯ НА МІСЦІ ПОДІЇ МОБІЛЬНИХ ТЕРМІНАЛІВ (СТІЛЬНИКОВИХ РАДІОТЕЛЕФОНІВ)

Мета статті полягає у висвітленні теоретико-прикладних підходів до правового забезпечення дій слідчих під час розслідування кримінальних правопорушень з отримання інформації з мобільних терміналів (стільникових радіотелефонів), виявлених на місці події, за допомогою технічних можливостей апаратно-програмного комплексу Cellebrite UFED. ***Методологія***. З огляду на специфіку об'єкта та предмета дослідження обрано методологічний інструментарій. Методологічну основу становить діалектичний підхід до аналізу проблематики документування та фіксування на місці події доказів, зважаючи на можливості апаратно-програмного комплексу Cellebrite UFED. Під час дослідження використано систему методів наукового пізнання: формальної логіки (абстрагування, логіки, індукції, дедукції, синтез) – для з'ясування змісту розглядуваних питань; теоретичний – у процесі дослідження наукової та навчально-методичної літератури; моделювання – для розроблення й упровадження в практику послідовності дій слідчих під час розслідування кримінальних правопорушень. ***Наукова новизна***. Запропоновано послідовність дій слідчого, якщо на місці події виявлено мобільний термінал (стільниковий радіотелефон), і порядок вилучення інформації (комп'ютерних даних) з цього пристрою за допомогою технічних можливостей апаратно-програмного комплексу Cellebrite UFED. ***Висновки***. Розглянуто дії слідчого, коли на місці події виявлений мобільний термінал (стільниковий радіотелефон), що зумовлює необхідність використання спеціальних знань. Профіль і кваліфікація фахівця, якого потрібно залучити до огляду мобільного термінала (стільникового радіотелефона), визначається залежно від мети і завдань слідчої (розшукової) дії, зважаючи на встановлені первинні дані про характер кримінального правопорушення. Запропоновано процесуальний порядок отримання інформації (комп'ютерних даних) із мобільного термінала (стільникового радіотелефона), що передбачає створення «образу» / електронного звіту наявної інформації, який записують на цифровий носій у вигляді файлу, закріплюють електронною міткою у вигляді контрольної суми. Надані науково-методичні рекомендації у процесі викладення основного матеріалу можуть становити методологічне підґрунтя ефективного виявлення та розслідування кримінальних правопорушень зазначеної спрямованості, зважаючи на те, що в реаліях сьогодення практики, а також наукова спільнота плідно працюють над новими програмними рішеннями, розробляють інноваційні методології проведення окремих криміналістичних досліджень, започатковують новітні технології.

Ключові слова: розслідування кримінального правопорушення; комп'ютерні дані; протокол; мобільний термінал; стільниковий радіотелефон; оперативно-технічний підрозділ; спеціаліст; спеціальні знання.

Вступ

Сучасні комп'ютери й 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 здійснюють 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, пов'язаної з повсякденною життєдіяльністю людини.

З огляду на це для з'ясування обставин вчинення кримінального правопорушення та встановлення істини у кримінальному провадженні (Pchelina, 2020; Yukhno, 2021, s. 269) постає нагальна потреба в отримані даних з електронних інформаційних пристроїв і систем. Адже 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 і зважаючи на реалії сьогодення законодавець увів до Кримінального процесуального кодексу України такі слідчі (розшукові) дії, як зняття інформації з електронних інформаційних систем (Kushpit, 2021) та обстеження на місці події мобільних терміналів.

Правові та криміналістичні основи фіксування криміналістично значущої інформації розробляли, зокрема, П. П. Артеменко, В. П. Бахін, В. Г. Гончаренко, О. В. Золотар, А. В. Іщенко,

В. О. Коновалова, В. К. Лисиченко, М. П. Молибога, І. В. Пиріг, М. В. Салтевський, М. Я. Сегай, В. Ю. Шепітько, М. Г. Щербаковський. Теоретико-прикладні підходи до розуміння електронних (цифрових) доказів та визначення їх місця в системі засобів доказування, використання електронних відображень як доказ у кримінальному провадженні вивчали В. Д. Гавловський, М. В. Гуцалюк, О. Г. Козицька, Р. Стойкова (Stoykova, 2021), В. Г. Хахановський, Г. Хорсман (Horsman, 2018), Д. М. Цехан, С. С. Чернявський та ін. Сьогодні науковці та практики, зарубіжні колеги активно висвітлюють, серед інших, питання так званої цифрової криміналістики (Satpathy, & Mohanty (Eds.), 2020; Easttom, 2021; Gogolin (Ed.), 2021; Shepitko, 2021; Shepitko, V., & Shepitko, M., 2021; Holt et al., 2022; Kaushik et al. (Eds.), 2022; Kolodina, & Fedorova, 2022; Moustafa, 2022; Stepaniuk, & Perlin, 2022). Досліджують проблеми залучення як спеціалістів працівників підрозділів, що здійснюють оперативно-розшукову діяльність (Pyrih, 2019); обмеження прав особи під час вилучення цифрових джерел доказової інформації у кримінальному провадженні (Demura, Klepka, & Krytska, 2020); окремі аспекти залучення спеціалістів для оперативно-розшукового документування (Sakovskyi, 2020); втручання у приватне спілкування шляхом зняття інформації з електронних інформаційних систем (Kushpit, 2021). Вивчають види електронних доказів у цивільному процесі (Chvankin, 2020); судову практику щодо допустимості доказів, отриманих у результаті проведення негласних слідчих (розшукових) дій (Drozd, 2020); виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням засобів стільникового радіозв'язку (Klymchuk, & Kuntii, 2020); «електронний доказ» під час обшуку (Pertsova-Todorova, 2020); застосування техніко-криміналістичних засобів при проведенні обшуку під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, особливості застосування техніко-криміналістичних засобів при проведенні окремих слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Teplytskyi, 2020a, 2020b); сутність електронної (цифрової) інформації як джерела доказів у кримінальному провадженні (Hutsaliuk, & Antoniuk, 2021); стан наукових досліджень у сфері електронних відображень у кримінальному провадженні (Hrebenkova, 2021); доказування у кримінальному провадженні на підставі електронних доказів (Dehtiarova, 2021); електронну інформацію як докази (Siemko, & Krakhmalov, 2021); теоретико-методологічну модель криміналістики та її нові напрями (Shepitko, 2021); сучасний стан і формування доктрини криміналістики та судової експертизи (Shepitko, & Shepitko, 2021); використання знань криміналістики у діяльності органів досудового розслідування і дізнання у протидії кримінальній протиправності (Yukhno, 2021); правові засади використання спеціальних знань під час інформаційного забезпечення досудового розслідування (Kovalova, 2022); особливості вилучення за допомогою технічних засобів інформації з мобільних терміналів радіозв'язку (смартфонів) під час кримінального провадження (Lisnichenko, 2022); процесуальні особливості отримання доказів під час слідчих (розшукових) дій (Rohatynska, & Tsitsiura, 2022).

Проте наразі бракує досліджень із проблематики отримання інформації (комп'ютерних даних) із мобільних терміналів (стільникових радіотелефонів), виявлених на місці події під час розслідування кримінальних правопорушень, що й зумовлює актуальність обраної тематики, визначаючи подальші напрями наших наукових розробок.

Мета й завдання дослідження

Мета статті – висвітлити теоретико-прикладні підходи до правового забезпечення дій слідчих під час розслідування кримінальних правопорушень з отримання інформації з мобільних терміналів (стільникових радіотелефонів), виявлених на місці події, за допомогою технічних можливостей апаратно-програмного комплексу Cellebrite UFED.

Для досягнення цієї мети потрібно вирішити такі завдання:

визначити особливості дій слідчо-оперативної групи з отримання інформації (комп'ютерних даних) із мобільного термінала (стільникового радіотелефона) на місці події;

запропонувати порядок процесуального оформлення отриманої інформації (комп'ютерних даних) із мобільного термінала (стільникового радіотелефона) на місці події;

надати відповідні науково-методичні рекомендації в контексті цього дослідження.

Виклад основного матеріалу

Проведення слідчих (розшукових) дій на місці події здійснюють із метою виявлення, оцінювання та дослідження слідів кримінального правопорушення, інших речей, що містять джерело доказової інформації, з'ясування обстановки кримінального правопорушення, інших обставин, що мають значення для кримінального провадження (Drozd, 2020; Rohatynska, & Tsitsiura, 2022). При цьому слідчий застосовує наявний арсенал

науково-технічних досягнень (Shepitko, & Shepitko, 2021; Yukhno, 2021; Karthikeyan, Pande, & Sarveshwaran (Eds.), 2023), оскільки несе відповідальність за перебіг досудового розслідування та, якщо йти логікою деяких науковців (Korcheva, 2020), його ефективність.

У разі виявлення та вилучення мобільних терміналів на місці події слідчий ініціює застосування апаратно-програмного комплексу Cellebrite UFED (Harris, & Lee, 2019; Holt, Bossler, & Seigfried-Spellar, 2022), який використовує у межах:

проведення такої слідчої (розшукової) дії, як огляд місцевості, приміщення, *речей*, документів і *комп'ютерних даних* (ст. 237 «Огляд» КПК України) – для огляду мобільного термінала (стільникового радіотелефона) та/або sim-картки;

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

Розгляньмо ці напрями докладніше.

Після надходження до органу, підрозділу поліції інформації про вчинення кримінального правопорушення та внесення інформації до Єдиного реєстру досудових розслідувань під керівництвом начальника органу, підрозділу поліції здійснюють комплекс першочергових заходів і 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, яку підозрюють у вчиненні кримінального правопорушення і у неї виявлений мобільний термінал, слідчий у складі слідчо-оперативної групи (далі – СОГ) ініціює таку слідчу (розшукову) дію, як огляд місцевості, приміщення, речей, документів та комп'ютерних даних (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 237) з метою виявлення та фіксування відомостей про обставини вчинення кримінального правопорушення. При цьому здійснюють не тільки зовнішній 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 (Klymchuk, & Kuntii, 2020). Зважаючи на технічну особливість цього пристрою, зумовлену його роботою (Kobets et al., 2004), та з метою одержання допомоги з питань, що потребують для таких дій спеціальних знань, слідчий, прокурор до участі в цьому огляді може запросити спеціаліста (Pyrih, 2019; Sakovskyi, 2020; Teplytskyi, 2020a, 2020b). У розглядуваному контексті дуже цікавий досвід зарубіжних колег (in particular, Pawlaszczyk, & Hummert, 2021; Hummert, & Pawlaszczyk, 2022; Spranger et al., 2022), які працюють над новими програмними рішеннями, розробляють інноваційні методології проведення окремих криміналістичних досліджень, започатковують новітні технології.

Зазвичай до зазначених дій слідчий залучає працівника оперативно-технічного підрозділу як спеціаліста (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 237, ch. 3; st. 71). При цьому спеціаліст зобов'язаний «прибути за викликом до слідчого, дізнавача, прокурора, суду і мати при собі необхідні технічне обладнання, пристрої та прилади» (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 71, ch. 5, p. 1). Тому слідчий інформує з місця події свого керівника про необхідність залучення працівника оперативно-технічного підрозділу з апаратно-програмним комплексом Cellebrite UFED (Leonov, & Nadizhko, 2020, s. 187). Участь працівника оперативно-технічного підрозділу слідчий фіксує в протоколі огляду предмета.

Для поглибленого розуміння відповідної слідчої (розшукової) дії, пов'язаної з технічною особливістю роботи мобільного термінала, 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. Зазвичай такі дії на місці події у складі СОГ здійснює інспектор-криміналіст (*Ministerstvo vnutrishnikh sprav Ukrainy*, 2017, Lypen 07, Instruktsii z orhanizatsii vzaiemodii). Згідно з положеннями базового міжнародного нормативного документа, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю (*Rada Yevropy*, 2001, Lystopad 23, Konventsiia pro kiberzlochynnist, st. 1), комп'ютерні дані – «будь-яке представлення 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». Тобто комп'ютерні дані містять як інформацію, так і програму для виконання певних дій комп'ютерної системи. Водночас дані – це інформація у придатній для автоматизованого

оброблення її засобами обчислювальної техніки, технічними та програмними засобами формі (*Verkhovna Rada Ukrainy*, 2020, Hruden 16, Pro elektronni komunikatsii, st. 2, ch. 1, p. 20). А електронні дані – будь-яка інформація в електронній формі (*Verkhovna Rada Ukrainy*, 2017, Zhovten 05, Pro elektronni dovirchi posluhy, st. 1, ch. 1, p. 13). Отже, у нашому випадку, дані – це інформація, представлена в електронному вигляді. У галузі криміналістики науковці поняття «електронні дані», «комп'ютерні дані» співвідносять із поняттями «комп'ютерна інформація», «цифрова інформація» (Khakhanovskyi, & Hutsaliuk, 2019; Teplytskyi, 2020a, 2020b; Hutsaliuk, & Antoniuk, 2021). 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 виявленого та вилученого слідчим стільникового радіотелефона, тобто інформації, не порушуючи слідів пальців рук на корпусі цього мобільного термінала для подальшого дослідження, та створює «образ» / електронний звіт наявної інформації (див. рис. 1). 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 в подальшому унеможливлює додаткові запитання зі сторони захисту під час судового розгляду) у вигляді файлу, закріплює електронною міткою у вигляді контрольної суми (hesh symma) із використанням алгоритму SHA-1 (SHA-2 або MD5) (див. рис. 2, 3). 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, а також зважаючи на позицію, витлумачену Верховним Судом, електронний підпис прирівняно до власноручного (*Verkhovna Rada Ukrainy*, 2017, Zhovten 05, Pro elektronni dovirchi posluhy, st. 1, p. 12; *Verkhovnyi Sud. Kasatsiinyi hospodarskyi sud*, 2021, Sichen 29, Pro stiahnennia koshtiv u sumi 525 736,50 hrn: postanova u spravi № 922/51/20, rozd. 8, p. 8.33).

Огляд комп'ютерних даних проводять слідчий, прокурор, 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 в паперовій формі) (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 237, ch. 2, abz. 2).

За результатами огляду слідчий складає протокол (st. 104). До протоколу як додаток долучають стільниковий радіотелефон, матеріальний носій інформації, підписаний працівником оперативно-технічного підрозділу алгоритмом хешування SHA-1 або SHA-2, MD5 з відомостями, отриманими під час огляду інформації з мобільних терміналів (стільникових радіотелефонів) та/або sim-карток (st. 105). Протокол підписують (104, ch. 5) усі учасники, які брали участь у проведенні процесуальної дії (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy).

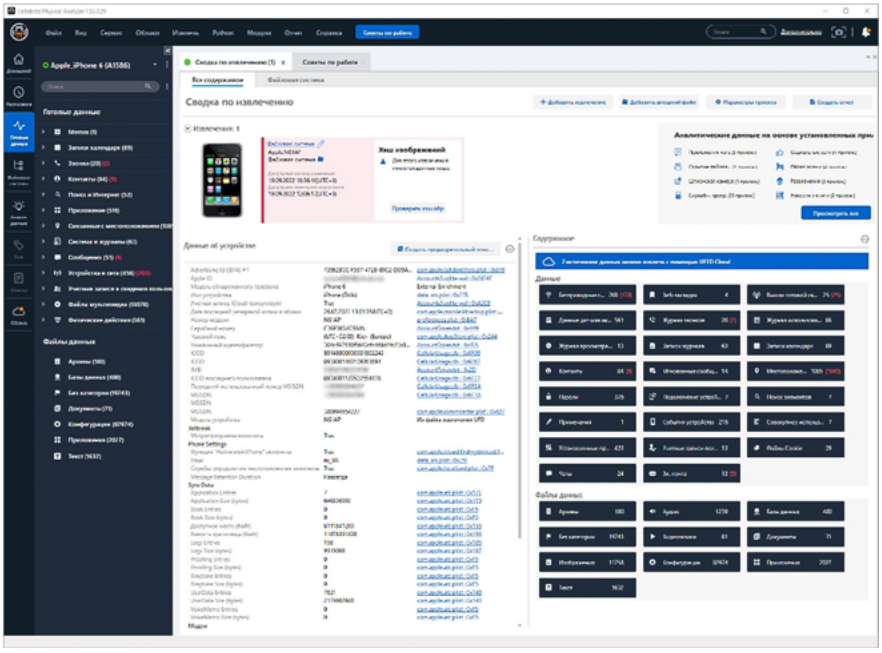

Рис. 1
Скриншот екрана апаратно-програмного комплексу Cellebrite UFED Touch 2 Ultimate із зображенням відкритого «образу»

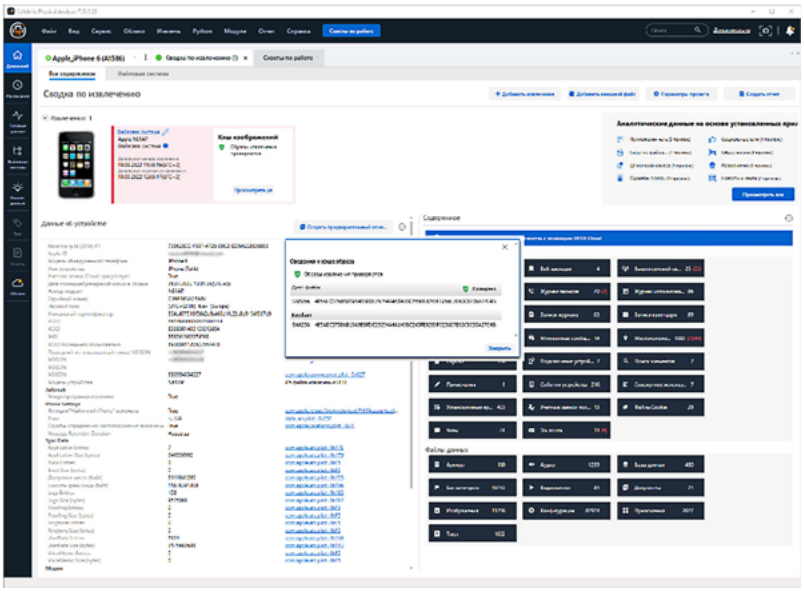

Рис. 2
Скриншот екрана апаратно-програмного комплексу Cellebrite UFED Touch 2 Ultimate із зображенням підрахованої хеш-суми

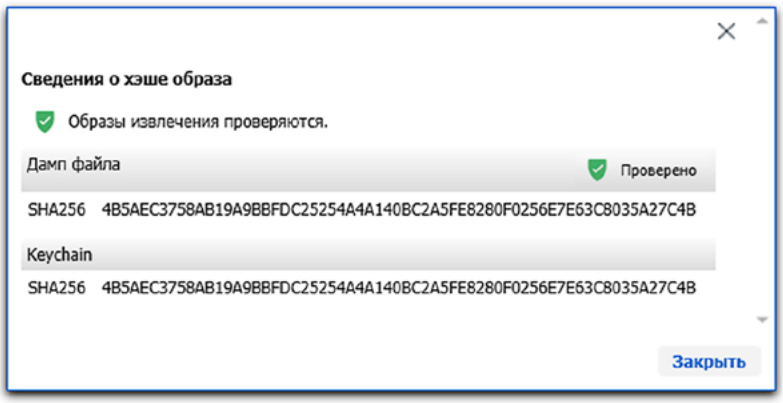

Рис. 3
Скриншот екрана апаратно-програмного комплексу Cellebrite UFED Touch 2 Ultimate із зображенням окремої хеш-суми «образу»

Розглядаючи протокольне оформлення доказової бази, слід зауважити, що відповідно до кримінального процесуального законодавства України джерелами доказів (st. 84) є показання, речові докази, документи (матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації, у тому числі комп'ютерні дані, тощо – st. 99, ch. 2, p. 1), висновки експерта (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy).

Водночас на практиці інколи постають юридичні ситуації, коли захисник опротестовує дії слідчого щодо неправомірності огляду стільникового радіотелефона 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.

Проте цю ситуацію розтлумачує Верховний Суд (*Verkhovnyi Sud. Kasatsiinyi kryminalnyi sud*, 2020, Kviten 09, Postanova u spravi No 727/6578/17 provadzhennia № 51-4494 km 19), тобто 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 із подоланням системи логічного захисту, при цьому не вбачаючи жодних порушень вимог кримінального процесуального закону під час дослідження інформації, яка була наявна в мобільному телефоні, шляхом увімкнення телефона й огляду текстових повідомлень, які в ньому містилися (*листування в телеграм-каналі*) та доступ до яких не був пов'язаний із наданням володільцем відповідного сервера (оператором мобільного зв'язку) доступу до електронних інформаційних систем. За таких обставин Верховний Суд не вбачає жодних порушень вимог кримінального процесуального закону під час огляду цього кримінального провадження.

Коментуючи рішення Верховного Суду, розгляньмо поняття мобільного телефона, а саме стільникового радіотелефона як мобільного термінала. Відповідно до законодавства України у сферах електронних комунікацій і радіочастотного спектра мобільним зв'язком вважають «електронні комунікації із застосуванням радіотехнологій, під час яких кінцеве обладнання хоча б одного зі споживачів може вільно переміщатися в межах усіх пунктів закінчення електронної комунікаційної мережі» (st. 2, p. 59). Разом із тим під кінцевим (термінальним) обладнанням розуміють «обладнання, призначене для з'єднання з кінцевим пунктом електронної комунікаційної мережі з метою забезпечення доступу до електронних комунікаційних послуг» (st. 2, p. 41), а електронною комунікаційною послугою є «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» (st. 2, p. 27) (*Verkhovna Rada Ukrainy*, 2020, Hruden 16, Pro elektronni komunikatsii). 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.

У межах кримінального провадження під час проведення такої слідчої (розшукової) дії, як обшук житла чи іншого володіння особи, обшук особи (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 236) для доступу до комп'ютерних систем або їх частин, мобільних терміналів (стільникових радіотелефонів) та/або sim-карток також залучають спеціаліста для огляду мобільного термінала (стільникового радіотелефона) і sim-картки безпосередньо на місці обшуку з подальшим його оглядом.

Для здійснення відповідної процесуальної дії слідчий залучає працівника оперативно-технічного підрозділу як спеціаліста (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 236, ch. 1; st. 71). У такому разі слідчий виносить відповідну постанову (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 110, ch. 3), а до оперативно-технічного підрозділу надсилають відповідний лист про необхідність проведення обшуку та, якщо буде виявлено стільниковий радіотелефон, його огляду працівником оперативно-технічного підрозділу, у якому зазначають дату та місце проведення огляду (без зазначення прізвища).

Законодавець (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy) передбачив й інші процесуальні дії в цьому напрямі:

«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» (st. 236, ch. 6, abz. 1);

«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» (st. 236, ch. 6, abz. 2);

«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» (st. 236, ch. 6, abz. 3);

«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» (st. 236, ch. 7);

«обшук житла чи іншого володіння особи на підставі ухвали слідчого судді в обов'язковому порядку фіксується за допомогою аудіо- та відеозапису» (st. 236, ch. 10).

У разі виявлення стільникового радіотелефона та/або sim-картки під час обшуку приміщення порядок застосування апаратно-програмного комплексу Cellebrite UFED, вилучення інформації з мобільного термінала та подальша процедура її документування аналогічні процесуальній дії з огляду.

За потреби слідчий направляє цифровий носій зі створеним «образом» / електронним звітом вилученого стільникового радіотелефона до

оперативно-технічного підрозділу для аналізування вилученої зі створеного «образу» інформації.

Наукова новизна

Запропоновано й обґрунтовано послідовність дій слідчого, якщо на місці події виявлено мобільний термінал (стільниковий радіотелефон), і порядок вилучення інформації (комп'ютерних даних) із цього пристрою за допомогою технічних можливостей апаратно-програмного комплексу Cellebrite UFED.

Висновки

1. Розглянуто дії слідчого, коли на місці події виявлено мобільний термінал (стільниковий радіотелефон), що зумовлює необхідність використання спеціальних знань. Профіль і кваліфікація фахівця, якого потрібно залучити до огляду мобільного термінала (стільникового радіотелефона), визначається залежно від мети і завдань слідчої (розшукової) дії, зважаючи на встановлені первинні дані про характер кримінального правопорушення.

2. Запропоновано процесуальний порядок отримання інформації (комп'ютерних даних) із мобільного термінала (стільникового радіотелефона), що передбачає створення «образу» / електронного звіту наявної інформації, який записують на цифровий носій у вигляді файлу, закріплюють електронною міткою у вигляді контрольної суми.

3. Надані науково-методичні рекомендації у процесі викладення основного матеріалу можуть становити методологічне підґрунтя ефективного виявлення та розслідування кримінальних правопорушень зазначеної спрямованості, зважаючи на те, що в реаліях сьогодення практики, а також наукова спільнота плідно працюють над новими програмними рішеннями, розробляють інноваційні методології проведення окремих криміналістичних досліджень, започатковують новітні технології.

References

Chvankin, S. (2020). Vydy elektronnykh dokaziv u tsyvilnomu protsesi [Types of electronic evidence in civil procedure]. *Knowledge, Education, Law, Management, 3*(31), vol. 2, 259–265 [in Ukrainian]. DOI: https://doi.org/10.51647/kelm.2020.3.2.45

Dehtiarova, O. (2021). Dokazuvannia u kryminalnomu provadzhenni na pidstavi elektronnykh dokaziv [Evidence in criminal proceedings on the basis of electronic evidence]. *Yurydychnyi visnyk, 6*, 273–278 [in Ukrainian]. DOI: https://doi.org/10.32837/yuv.v0i6.2292

Demura, M. I., Klepka, D. I., & Krytska, I. O. (2020). Shchodo obmezhennia prav osoby pid chas vyluchennia tsyfrovykh dzherel dokazovoi informatsii u kryminalnomu provadzhenni [Restriction of personal rights when removing digital sources of evidence in criminal proceedings]. *Forum Prava, 60*(1), 37–46 [in Ukrainian]. DOI: https://doi.org/10.5281/zenodo.3577546

Drozd, V. (2020). Sudova praktyka shchodo dopustymosti dokaziv, otrymanykh u rezultati provedennia nehlasnykh slidchykh (rozshukovykh) dii [Judicial practice on the admissibility of evidence obtained during the covert investigative activities]. *Pidpryiemnytstvo, hospodarstvo i pravo, 9,* 185–190 [in Ukrainian]. DOI: https://doi.org/10.32849/2663-5313/2020.9.32

Easttom, C. (2021). *An In-Depth Guide to Mobile Device Forensics* (1st ed.). CRC Press. DOI: https://doi.org/10.1201/9781003118718

Gogolin, G. (Ed.). (2021). *Digital Forensics Explained* (2nd ed.). CRC Press. DOI: https://doi.org/10.1201/9781003049357

Harris, H. A., & Lee, H. C. (2019). *Introduction to Forensic Science and Criminalistics* (2nd ed.). CRC Press. DOI: https://doi.org/10.4324/9781315119175

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge. DOI: https://doi.org/10.4324/9780429343223

Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers & Security, 73*, 294–306. DOI: https://doi.org/10.1016/j.cose.2017.11.009

Hrebenkova, M. S. (2021). Stan naukovykh doslidzhen v sferi elektronnykh vidobrazhen u kryminalnomu provadzhenni [Situation of scientific research in the sphere of electronic mapping in criminal proceedings]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo, 67*, 267–272 [in Ukrainian]. DOI: https://doi.org/10.24144/2307-3322.2021.67.51

Hummert, C., & Pawlaszczyk, D. (2022). *Mobile Forensics – The File Format Handbook*: *Common File Formats and File Systems Used in Mobile Devices*. Springer. DOI: 10.1007/978-3-030-98467-0

Hutsaliuk, M. V., & Antoniuk, P. Ye. (2021). Shchodo sutnosti elektronnoi (tsyfrovoi) informatsii yak dzherela dokaziv u kryminalnomu provadzhenni [The essence of digital informationas a source of evidence in criminal proceedings]. *Kryminalistychnyi visnyk, 33*(1), 37–49 [in Ukrainian]. DOI: https://doi.org/10.37025/1992-4437/2020-33-1-37

Karthikeyan, P., Pande, H. M., & Sarveshwaran, V. (Eds.). (2023). *Artificial Intelligence and Blockchain in Digital Forensics* (1st ed.). River Publishers.
DOI: https://doi.org/10.1201/9781003374671

Kaushik, K., Tanwar, R., Dahiya, S., Bhatia, K. K., & Wu, Y. (Eds.). (2022). *Unleashing the Art of Digital Forensics* (1st ed.). Chapman and Hall/CRC.
DOI: https://doi.org/10.1201/9781003204862

Khakhanovskyi, V. H., & Hutsaliuk, M. V. (2019). Osoblyvosti vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [The peculiarities of digital evidence use in criminal proceedings]. *Kryminalistychnyi visnyk, 1*(31), 14–20 [in Ukrainian].
DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13

Klymchuk, M. P., & Kuntii, A. I. (2020). Vyiavlennia ta vyluchennia slidiv kryminalnykh pravoporushen, uchynenykh iz vykorystanniam zasobiv stilnykovoho zviazku [Detection and extraction of traces of criminal offenses committed with the use of cellular communication means]. *Sotsialno-pravovi studii, 3*(9), 111–118 [in Ukrainian].
DOI: 10.32518/2617-4162-2020-3-111-118

Kobets, M. V., Lanevskyi, E. V., & Yakovenko, O. V. (2004). *Zasoby ta systemy zviazku OVS*: navch. posib. Kyiv: Natsionalna akad. vnutr. sprav Ukrainy. 97 s. http://elar.naiau.kiev.ua/jspui/bitstream/123456789/18998/1/Kobets%20M.V.%20Zasoby%20t%D0%B0%20systemy%20zvaiyzku.pdf [in Ukrainian].

Kolodina, A. S., & Fedorova, T. S. (2022). Tsyfrova kryminalistyka: problemy teorii i praktyky [Digital forensics: problems of theory and practice]. *Yurydychnyi naukovyi elektronnyi zhurnal, 4,* 378–380 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2022-4/90

Korcheva, T. V. (2020). Do pytannia vyznachennia poniattia efektyvnosti dosudovoho rozsliduvannia. In *Legal science, legislation and law enforcement practice: regularities and development trends*: proceedings international scientific and practical conference (October 30–31) (pp. 355–359). Lublin: Baltija Publishing [in Ukrainian].
DOI: 10.30525/978-9934-588-92-1-89

Kovalova, O. V. (2022). Pravovi zasady vykorystannia spetsialnykh znan pid chas informatsiinoho zabezpechennia dosudovoho rozsliduvannia [Legal principles of using special knowledge during information provision of investigative investigation]. *Kyivskyi chasopys prava, 1*, 168–175 [in Ukrainian].
DOI: https://doi.org/10.32782/klj/2022.1.26

Kushpit, V. P. (2021). Vtruchannia u pryvatne spilkuvannia shliakhom zniattia informatsii z elektronnykh informatsiinykh system [Interference in private communication by removal information from electronic information systems]. *Nashe Pravo, 4*, 89–94 [in Ukrainian].
DOI: https://doi.org/10.32782/np.2021.4.13

Leonov, B. D., & Nadizhko, M. M. (2020). Naukovo-tekhnichne zabezpechennia sudovo-ekspertnoi diialnosti: suchasnyi stan ta perspektyvy [Scientific and technical support of forensic expert activities: current status and prospects]. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo», 2*(55), 184–190 [in Ukrainian].
DOI: 10.18372/2307-9061.55.14793

Lisnichenko, D. V. (2022). Osoblyvosti vyluchennia za dopomohoiu tekhnichnykh zasobiv informatsii z mobilnykh terminaliv zviazku (smartfoniv) pid chas kryminalnoho provadzhennia [Features of extraction by technical means of information from mobile communication terminals (smartphones) during criminal proceedings]. *Pivdennoukrainskyi pravnychyi chasopys, 1–2*, 120–125 [in Ukrainian].
DOI: https://doi.org/10.32850/sulj.2022.1-2.22

Ministerstvo vnutrishnikh sprav Ukrainy. (2017, Lypen 07). *Instruktsii z orhanizatsii vzaiemodii orhaniv dosudovoho rozsliduvannia z inshymy orhanamy ta pidrozdilamy Natsionalnoi politsii Ukrainy v zapobihanni kryminalnym pravoporushenniam, yikh vyiavlenni ta rozsliduvanni*: zatv. nakazom No 575. https://zakon.rada.gov.ua/laws/show/z0937-17#Text [in Ukrainian].

Moustafa, N. (2022). *Digital Forensics in the Era of Artificial Intelligence* (1st ed.). CRC Press.
DOI: https://doi.org/10.1201/9781003278962

Pawlaszczyk, D., & Hummert, C. (2021). Making the Invisible Visible – Techniques for Recovering Deleted SQLite Data Records. *International Journal of Cyber Forensics and Advanced Threat Investigations, 1*(1–3), 27–41.
DOI: 10.46386/ijcfati.v1i1-3.17

Pchelina, O. V. (2020). Obstavyny, shcho pidliahaiut ziasuvanniu pid chas rozsliduvannia kryminalnykh pravoporushen, i yikhnie mistse u strukturi okremoi kryminalistychnoi metodyky [Circumstances to be clarified during the investigation of criminal offenses and their place in the structure of a separate forensic methodology]. *Prykarpatskyi yurydychnyi visnyk, 2*(31), 187–190 [in Ukrainian].
DOI: https://doi.org/10.32837/pyuv.v0i2(31).590

Pertsova-Todorova, L. (2020). «Elektronnyi dokaz» pid chas obshuku ["Electronic evidence" during the search]. *Pidpryiemnytstvo, hospodarstvo i pravo, 6*, 243–247 [in Ukrainian].
DOI: https://doi.org/10.32849/2663-5313/2020.6.41

Pyrih, I. V. (2019). Involvement of specialists in investigative activities in the investigation of criminal offenses. In *Realities and prospects for the development of the rule-of-law state in Ukraine and worldwide* (pp. 93–122). Lviv-Torun: Liha-Pres.

DOI: https://doi.org/10.36059/978-966-397-207-7/93-122

Rada Yevropy. (2001, Lystopad 23). *Konventsiia pro kiberzlochynnist*: ratyfikovana iz zasterezhenniamy i zaiavamy Zakonom Ukrainy No 2824-IV vid 07.09.2005. https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian].

Rohatynska, N. Z., & Tsitsiura, O. I. (2021). Protsesualni osoblyvosti otrymannia dokaziv pid chas slidchykh (rozshukovykh) dii [Procedural features of obtaining evidences in the course of carrying out investigation]. *Znannia yevropeiskoho prava, 6*, 78–82 [in Ukrainian].
DOI: 10.32837/chern.v0i6.304

Sakovskyi, A. A. (2020). Okremi aspekty zaluchennia spetsialistiv dlia operatyvno-rozshukovoho dokumentuvannia [Certain aspects of involvement of specialists for operational and examination documentation]. *Yurydychna nauka,* 5(107), 190–195 [in Ukrainian].
DOI: https://doi.org/10.32844/2222-5374-2020-107-5-1.23

Satpathy, S., & Mohanty, S. (Eds.). (2020). *Big Data Analytics and Computing for Digital Forensic Investigations* (1st ed.). CRC Press.
DOI: https://doi.org/10.1201/9781003024743

Shepitko, V. (2021). Teoretyko-metodolohichna model kryminalistyky ta yii novi napriamy [Theoretical and methodological model of criminalistics and its new directions]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky, 25*(3), 9–20 [in Ukrainian].
DOI: https://doi.org/10.32353/khrife.3.2021.02

Shepitko, V., & Shepitko, M. (2021). Doktryna kryminalistyky ta sudovoi ekspertyzy: formuvannia, suchasnyi stan i rozvytok v Ukraini [Doctrine of criminalistics and forensic examination: formation, current state and development in Ukraine]. *Pravo Ukrainy, 8*, 12–27 [in Ukrainian].
DOI: 10.33498/louu-2021-08-012

Siemko, M. O., & Krakhmalov, O. V. (2021). Elektronna informatsiia yak dokazy [Electronic information as evidence]. *Visnyk Natsionalnoho tekhnichnoho universytetu «KhPI». Seriia: Aktualni problemy rozvytku ukrainskoho suspilstva, 1*, 48–51 [in Ukrainian].
DOI: 10.20998/2227-6890.2021.1.07

Spranger, M., Xi, J., Jaeckel, L., Felser, J., & Labudde, D. (2022). MoNA: A Forensic Analysis Platform for Mobile Communication. *Künstliche Intelligenz, 36*, 163–169.
DOI: https://doi.org/10.1007/s13218-022-00762-w

Stepaniuk, R. L., & Perlin, S. I. (2022). Tsyfrova kryminalistyka y udoskonalennia systemy kryminalistychnoi tekhniky v Ukraini [Digital forensics and improvement of the forensic technology system in Ukraine]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka, 3*(99), 283–284 [in Ukrainian].
DOI: https://doi.org/10.33766/2524-0323.99.283-284

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review, 42*, 105575.
DOI: https://doi.org/10.1016/j.clsr.2021.105575

Teplytskyi, B. B. (2020a). Zastosuvannia tekhniko-kryminalistychnykh zasobiv pry provedenni obshuku pid chas rozsliduvannia zlochyniv u sferi vykorystannia kompiuteriv, system ta kompiuternykh merezh i merezh elektrozviazku [Application of criminal tools during a search during investigation of crimes in the field of use of computers, systems and computer networks and telecommunications networks]. *Yurydychna nauka, 2*(5(107), 151–157 [in Ukrainian].
DOI: 10.32844/2222-5374-2020-107-5-2.19

Teplytskyi, B. B. (2020b). Osoblyvosti zastosuvannia tekhniko-kryminalistychnykh zasobiv pry provedenni okremykh slidchykh (rozshukovykh) dii pid chas rozsliduvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku [Technical features of forensic products during certain investigative (detective) actions during the investigation of crimes in the use of computers systems and computer networks and telecommunication networks]. *Yurydychna nauka, 6*(108), 248–255 [in Ukrainian].
DOI: https://doi.org/10.32844/2222-5374-2020-108-6-1.30

Verkhovna Rada Ukrainy. (2012, Kviten 13). *Kryminalnyi protsesualnyi kodeks Ukrainy*: Zakon Ukrainy No 4651-VI. https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].

Verkhovna Rada Ukrainy. (2017, Zhovten 05). *Pro elektronni dovirchi posluhy*: Zakon Ukrainy No 2155-VIII. https://zakon.rada.gov.ua/laws/show/2155-19/ed20220101#top [in Ukrainian].

Verkhovna Rada Ukrainy. (2020, Hruden 16). *Pro elektronni komunikatsii*: Zakon Ukrainy No 1089-IX. https://zakon.rada.gov.ua/laws/show/1089-20#Text [in Ukrainian].

Verkhovnyi Sud. Kasatsiinyi hospodarskyi sud. (2021, Sichen 29). *Pro stiahnennia koshtiv u sumi 525 736,50 hrn*: postanova u spravi No 922/51/20. https://verdictum.ligazakon.net/document/94517830 [in Ukrainian].

Verkhovnyi Sud. Kasatsiinyi kryminalnyi sud. (2020, Kviten 09). *Postanova u spravi No 727/6578/17 provadzhennia № 51-4494 km 19*. https://zakononline.com.ua/court-decisions/show/88749345 [in Ukrainian].

Yukhno, O. O. (2021). Vykorystannia znan kryminalistyky u diialnosti orhaniv dosudovoho rozsliduvannia i diznannia u protydii zlochynnosti. In *Legal sciences: research and european innovations*: proceedings international scientific and practical conference (April 23–24) (pp. 268–273). Czestochowa: Baltija Publishing [in Ukrainian].
DOI: 10.30525/978-9934-26-074-2-71

Список використаних джерел

Чванкін, С. (2020). Види електронних доказів у цивільному процесі [Types of electronic evidence in civil procedure]. *Knowledge, Education, Law, Management, 3*(31), vol. 2, 259–265.
DOI: https://doi.org/10.51647/kelm.2020.3.2.45

Дегтярьова, О. (2021). Доказування у кримінальному провадженні на підставі електронних доказів [Evidence in criminal proceedings on the basis of electronic evidence]. *Юридичний вісник, 6*, 273–278.
DOI: https://doi.org/10.32837/yuv.v0i6.2292

Демура, М. І., Клепка, Д. І., & Крицька, І. О. (2020). Щодо обмеження прав особи під час вилучення цифрових джерел доказової інформації у кримінальному провадженні [Restriction of personal rights when removing digital sources of evidence in criminal proceedings]. *Форум Права, 60*(1), 37–46.
DOI: https://doi.org/10.5281/zenodo.3577546

Дрозд, В. (2020). Судова практика щодо допустимості доказів, отриманих у результаті проведення негласних слідчих (розшукових) дій [Judicial practice on the admissibility of evidence obtained during the covert investigative activities]. *Pidpryiemnytstvo, hospodarstvo i pravo, 9,* 185–190.
DOI: https://doi.org/10.32849/2663-5313/2020.9.32

Easttom, C. (2021). *An In-Depth Guide to Mobile Device Forensics* (1st ed.). CRC Press.
DOI: https://doi.org/10.1201/9781003118718

Gogolin, G. (Ed.). (2021). *Digital Forensics Explained* (2nd ed.). CRC Press.
DOI: https://doi.org/10.1201/9781003049357

Harris, H. A., & Lee, H. C. (2019). *Introduction to Forensic Science and Criminalistics* (2nd ed.). CRC Press.
DOI: https://doi.org/10.4324/9781315119175

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge.
DOI: https://doi.org/10.4324/9780429343223

Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers & Security, 73*, 294–306.
DOI: https://doi.org/10.1016/j.cose.2017.11.009

Гребенькова, М. С. (2021). Стан наукових досліджень в сфері електронних відображень у кримінальному провадженні [Situation of scientific research in the sphere of electronic mapping in criminal proceedings]. *Науковий вісник Ужгородського Національного Університету. Серія: Право, 67*, 267–272.
DOI: https://doi.org/10.24144/2307-3322.2021.67.51

Hummert, C., & Pawlaszczyk, D. (2022). *Mobile Forensics – The File Format Handbook*: *Common File Formats and File Systems Used in Mobile Devices*. Springer.
DOI: 10.1007/978-3-030-98467-0

Гуцалюк, М. В., & Антонюк, П. Є. (2021). Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні [The essence of digital informationas a source of evidence in criminal proceedings]. *Криміналістичний вісник*, *33*(1), 37–49.
DOI: https://doi.org/10.37025/1992-4437/2020-33-1-37

Karthikeyan, P., Pande, H. M., & Sarveshwaran, V. (Eds.). (2023). *Artificial Intelligence and Blockchain in Digital Forensics* (1st ed.). River Publishers.
DOI: https://doi.org/10.1201/9781003374671

Kaushik, K., Tanwar, R., Dahiya, S., Bhatia, K. K., & Wu, Y. (Eds.). (2022). *Unleashing the Art of Digital Forensics* (1st ed.). Chapman and Hall/CRC.
DOI: https://doi.org/10.1201/9781003204862

Хахановський, В. Г., & Гуцалюк, М. В. (2019). Особливості використання електронних (цифрових) доказів у кримінальних провадженнях [The peculiarities of digital evidence use in criminal proceedings]. *Криміналістичний вісник, 1*(31), 14–20.
DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13

Климчук, М. П., & Кунтій, А. І. (2020). Виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням засобів стільникового зв'язку [Detection and extraction of traces of criminal offenses committed with the use of cellular communication means]. *Соціально-правові студії, 3*(9), 111–118.
DOI: 10.32518/2617-4162-2020-3-111-118

Кобець, М. В., Ланевський, Е. В., & Яковенко, О. В. (2004). *Засоби та системи зв'язку ОВС:* навч. посіб. Київ: Національна акад. внутр. справ України. 97 с. http://elar.naiau.kiev.ua/jspui/bitstream/123456789/18998/1/Kobets%20M.V.%20Zasoby%20t%D0%B0%20systemy%20zvaiyzku.pdf

Колодіна, А. С., & Федорова, Т. С. (2022). Цифрова криміналістика: проблеми теорії і практики [Digital forensics: problems of theory and practice]. *Юридичний науковий електронний журнал, 4*, 378–380.
DOI: https://doi.org/10.32782/2524-0374/2022-4/90

Корчева, Т. В. (2020). До питання визначення поняття ефективності досудового розслідування. In *Legal science, legislation and law enforcement practice: regularities and development trends:* proceedings international scientific and practical conference (October 30–31) (pp. 355–359). Lublin: Baltija Publishing.

DOI: 10.30525/978-9934-588-92-1-89

Ковальова, О. В. (2022). Правові засади використання спеціальних знань під час інформаційного забезпечення досудового розслідування [Legal principles of using special knowledge during information provision of investigative investigation]. *Київський часопис права, 1, 168–175.*
DOI: https://doi.org/10.32782/klj/2022.1.26

Кушпіт, В. П. (2021). Втручання у приватне спілкування шляхом зняття інформації з електронних інформаційних систем [Interference in private communication by removal information from electronic information systems]. *Наше Право, 4*, 89–94.
DOI: https://doi.org/10.32782/np.2021.4.13

Леонов, Б. Д., & Надіжко, М. М. (2020). Науково-технічне забезпечення судово-експертної діяльності: сучасний стан та перспективи [Scientific and technical support of forensic expert activities: current status and prospects]. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право», 2*(55), 184–190.
DOI: 10.18372/2307-9061.55.14793

Лісніченко, Д. В. (2022). Особливості вилучення за допомогою технічних засобів інформації з мобільних терміналів зв'язку (смартфонів) під час кримінального провадження [Features of extraction by technical means of information from mobile communication terminals (smartphones) during criminal proceedings]. *Південноукраїнський правничий часопис, 1–2*, 120–125.
DOI: https://doi.org/10.32850/sulj.2022.1-2.22

Міністерство внутрішніх справ України. (2017, Липень 07). *Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні:* затв. наказом № 575. https://zakon.rada.gov.ua/laws/show/z0937-17#Text

Moustafa, N. (2022). *Digital Forensics in the Era of Artificial Intelligence* (1st ed.). CRC Press.
DOI: https://doi.org/10.1201/9781003278962

Pawlaszczyk, D., & Hummert, C. (2021). Making the Invisible Visible – Techniques for Recovering Deleted SQLite Data Records. *International Journal of Cyber Forensics and Advanced Threat Investigations, 1*(1–3), 27–41.
DOI: 10.46386/ijcfati.v1i1-3.17

Пчеліна, О. В. (2020). Обставини, що підлягають з'ясуванню під час розслідування кримінальних правопорушень, і їхнє місце у структурі окремої криміналістичної методики [Circumstances to be clarified during the investigation of criminal offenses and their place in the structure of a separate forensic methodology]. *Прикарпатський юридичний вісник, 2*(31), 187–190.
DOI: https://doi.org/10.32837/pyuv.v0i2(31).590

Перцова-Тодорова, Л. (2020). «Електронний доказ» під час обшуку ["Electronic evidence" during the search]. *Підприємництво, господарство і право, 6*, 243–247.
DOI: https://doi.org/10.32849/2663-5313/2020.6.41

Pyrih, I. V. (2019). Involvement of specialists in investigative activities in the investigation of criminal offenses. In *Realities and prospects for the development of the rule-of-law state in Ukraine and worldwide* (pp. 93–122). Lviv-Torun: Liha-Pres.
DOI: https://doi.org/10.36059/978-966-397-207-7/93-122

Рада Європи. (2001, Листопад 23). *Конвенція про кіберзлочинність:* ратифікована із застереженнями і заявами Законом України № 2824-IV від 07.09.2005. https://zakon.rada.gov.ua/laws/show/994_575#Text

Рогатинська, Н. З., & Ціцюра, О. І. (2021). Процесуальні особливості отримання доказів під час слідчих (розшукових) дій [Procedural features of obtaining evidences in the course of carrying out investigation]. *Знання європейського права, 6*, 78–82.
DOI: 10.32837/chern.v0i6.304

Саковський, А. А. (2020). Окремі аспекти залучення спеціалістів для оперативно-розшукового документування [Certain aspects of involvement of specialists for operational and examination documentation]. *Юридична наука, 5*(107), 190–195.
DOI: https://doi.org/10.32844/2222-5374-2020-107-5-1.23

Satpathy, S., & Mohanty, S. (Eds.). (2020). *Big Data Analytics and Computing for Digital Forensic Investigations* (1st ed.). CRC Press.
DOI: https://doi.org/10.1201/9781003024743

Шепітько, В. (2021). Теоретико-методологічна модель криміналістики та її нові напрями [Theoretical and methodological model of criminalistics and its new directions]. *Теорія та практика судової експертизи і криміналістики, 25*(3), 9–20.
DOI: https://doi.org/10.32353/khrife.3.2021.02

Шепітько, В., & Шепітько, М. (2021). Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні [Doctrine of criminalistics and forensic examination: formation, current state and development in Ukraine]. *Право України, 8*, 12–27.
DOI: 10.33498/louu-2021-08-012

Сємко, М. О., & Крахмальов, О. В. (2021). Електронна інформація як докази [Electronic information as evidence].

Вісник Національного технічного університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства, 1, 48–51.
DOI: 10.20998/2227-6890.2021.1.07

Spranger, M., Xi, J., Jaeckel, L., Felser, J., & Labudde, D. (2022). MoNA: A Forensic Analysis Platform for Mobile Communication. *Künstliche Intelligenz, 36*, 163–169.
DOI: https://doi.org/10.1007/s13218-022-00762-w

Степанюк, Р. Л., & Перлін, С. І. (2022). Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні [Digital forensics and improvement of the forensic technology system in Ukraine]. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, 3*(99), 283–284.
DOI: https://doi.org/10.33766/2524-0323.99.283-284

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review, 42*, 105575.
DOI: https://doi.org/10.1016/j.clsr.2021.105575

Теплицький, Б. Б. (2020a). Застосування техніко-криміналістичних засобів при проведенні обшуку під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку [Application of criminal tools during a search during investigation of crimes in the field of use of computers, systems and computer networks and telecommunications networks]. *Юридична наука*, *2*(5(107), 151–157.
DOI: 10.32844/2222-5374-2020-107-5-2.19

Теплицький, Б. Б. (2020b). Особливості застосування техніко-криміналістичних засобів при проведенні окремих слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [Technical features of forensic products during certain investigative (detective) actions during the investigation of crimes in the use of computers systems and computer networks and telecommunication networks]. *Юридична наука, 6*(108), 248–255.
DOI: https://doi.org/10.32844/2222-5374-2020-108-6-1.30

Верховна Рада України. (2012, Квітень 13). *Кримінальний процесуальний кодекс України:* Закон України № 4651-VI. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Верховна Рада України. (2017, Жовтень 05). *Про електронні довірчі послуги:* Закон України № 2155-VIII. https://zakon.rada.gov.ua/laws/show/2155-19/ed20220101#top

Верховна Рада України. (2020, Грудень 16). *Про електронні комунікації:* Закон України № 1089-IX. https://zakon.rada.gov.ua/laws/show/1089-20#Text

Верховний Суд. Касаційний господарський суд. (2021, Січень 29). *Про стягнення коштів у сумі 525 736,50 грн:* постанова у справі № 922/51/20. https://verdictum.ligazakon.net/document/94517830

Верховний Суд. Касаційний кримінальний суд. (2020, Квітень 09). *Постанова у справі № 727/6578/17 провадження № 51-4494 км 19*. https://zakononline.com.ua/court-decisions/show/88749345

Юхно, О. О. (2021). Використання знань криміналістики у діяльності органів досудового розслідування і дізнання у протидії злочинності. In *Legal sciences: research and european innovations*: proceedings international scientific and practical conference (April 23–24) (pp. 268–273). Czestochowa: Baltija Publishing.
DOI: 10.30525/978-9934-26-074-2-71

Стаття надійшла до редакції 18.11.2022

M. Kobets,
Cand. Sc. (Law), Senior Researcher,
Associate Professor of the Department
of Operational and Search Activities,
National Academy of Internal Affairs, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2233-0946
email: mv.kobets@ukr.net

INVESTIGATOR'S ACTIONS DURING THE DETECTION OF THE MOBILE TERMINALS (CELLULAR RADIO PHONES) AT THE SCENE

The purpose of the article is to highlight the theoretical and applied approaches to the legal support of the actions of investigators during the investigation of criminal offenses for obtaining information from mobile terminals (cellular radio phones) found at the scene, using the technical capabilities of the Cellebrite UFED hardware and software complex. ***Methodology***. Given the specifics of the object and subject of the study, the methodological toolkit was chosen. The methodological basis is a dialectical approach to the analysis of the problems of documenting and recording evidence at the scene, taking into account the capabilities of the Cellebrite UFED hardware and software complex. During the research, a system of methods of scientific knowledge was used: formal logic (abstraction, logic, induction, deduction, synthesis) – to clarify the content of the issues under consideration; theoretical – in the process of researching scientific and educational and methodological literature; modeling – for the development and implementation in practice of the sequence of actions of investigators during the investigation of criminal offenses. ***Scientific novelty***. The sequence of actions of the investigator, if a mobile terminal (cellular radio telephone) is found at the scene and the procedure for extracting information content (computer data) from this device, using the technical capabilities of the Cellebrite UFED hardware and software complex, are proposed. ***Conclusions***. The actions of the investigator were considered if a mobile terminal (cellular radio telephone) was found at the scene, the peculiarity of which is the need to use special knowledge. The profile and qualification of a specialist who must be involved in the examination of a mobile terminal (cellular radio telephone) is determined depending on the purpose and tasks of the investigative (search) action, taking into account the established primary data on the nature of the criminal offense. A procedural procedure for obtaining information (computer data) from a mobile terminal (cellular radio telephone) is proposed, during which an "image"/electronic report of the available information is created, which is recorded on a digital medium in the form of a file, and secured with an electronic tag in the form of a checksum. The provided scientific and methodological recommendations in the process of presenting the main material can form a methodological basis for the effective detection and investigation of criminal offenses of the specified orientation, taking into account the fact that in today's realities, practitioners, as well as the scientific community, are fruitfully working on new software solutions, developing innovative methodologies for conducting individual forensic researches, initiate the latest technologies.

Keywords: criminal investigation; computer data; protocol; mobile terminal; cellular radio telephone; operational and technical division; specialist; special knowledge.