**Кримінальний процес та криміналістика**

УДК 343.132 : 343.985

**DOI** https://doi.org/**10.5281/zenodo.16755828**

# Тактика обшуку мобільних терміналів систем зв'язку

**Коломійцев Сергій Олександрович**

науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі навчально-наукового інституту № 4,

Харківський національний університет внутрішніх справ,

м. Харків, Україна, https://orcid.org/0009-0006-7070-9471

**Прийнято: 16.07.2025 | Опубліковано: 26.07.2025**

***Анотація.*** *Метою дослідження є аналіз особливостей обшуку мобільних терміналів як джерела криміналістично значущої інформації в умовах зростання злочинів, скоєних із використанням інформаційних технологій, та визначення процесуальних, криміналістичних і технічних аспектів для забезпечення законності й ефективності досудового розслідування.*

*У роботі застосовано комплексний підхід, що включає аналіз положень Закону України «Про електронні комунікації» та Кримінального процесуального кодексу України, вивчення зарубіжного досвіду (зокрема Великобританії та США), а також узагальнення наукових джерел із криміналістичної тактики. Досліджено алгоритми проведення обшуку, огляду та експертизи мобільних пристроїв, а також технічні засоби, такі як спеціалізоване програмне забезпечення (EnCase, Oxygen, UFED).*

*Встановлено, що обшук мобільних терміналів охоплює процесуальну, криміналістичну та технічну складові. Визначено зміст даних, які містяться в мобільних пристроях: контакти, повідомлення, геолокація, історія браузерів, графічні файли тощо. Доведено, що недотримання процесуальних вимог під час доступу до приватної інформації може призвести до визнання отриманих даних неприпустимими доказами. Виявлено, що основними слідчими діями для збирання цифрової інформації є тимчасовий доступ до речей і документів, обшук, огляд та експертиза. Тактика обшуку поділяється на три етапи: підготовчий, робочий (із зовнішнім, конструктивним та інформаційним оглядом) і заключний. Проаналізовано особливості дослідження вмісту смартфонів, зокрема файлів, повідомлень, браузерів та картографічних сервісів, із наголосом на необхідності належної фіксації інформації (протокол, фото-, відеозйомка). Встановлено, що технічна складова передбачає використання спеціалізованого програмного забезпечення для аналізу даних, відновлення видалених файлів і фіксації цифрових слідів.*

*У висновках обґрунтовано важливість дотримання процесуальних норм під час обшуку мобільних терміналів для забезпечення законності та захисту особистих прав. Запропоновано вдосконалення тактики обшуку шляхом чіткого структурування етапів і використання сучасних технічних засобів. Результати можуть бути використані для вдосконалення практики досудового розслідування та розробки рекомендацій для слідчих і судових експертів.*

***Ключові слова:*** *кримінальне провадження, обшук, огляд, тимчасове вилучення майна, арешт майна, цифрова інформація, тактичні прийоми, дослідження вмісту смартфону.*

# Tactics of searching mobile terminals of communication systems

**Kolomiitsev Serhii**

Educational and Scientific Institute No. 4, Research Laboratory on the Problems of Information Technologies and Combating Crime in Cyberspace (researcher),

Kharkiv National University of Internal Affairs,

Kharkiv, Ukraine, https://orcid.org/0009-0006-7070-9471

***Abstract***. *The purpose of the study is to analyze the specifics of searching mobile terminals as sources of forensically significant information amid the increasing prevalence of crimes committed using information technologies, and to identify the procedural, forensic, and technical aspects to ensure the legality and effectiveness of pre-trial investigations.*

*A comprehensive approach was employed, including analysis of the provisions of the Law of Ukraine "On Electronic Communications" and the Criminal Procedure Code of Ukraine, examination of foreign practices (notably in the United Kingdom and the United States), and synthesis of scientific sources on forensic tactics. The study explored algorithms for conducting searches, inspections, and examinations of mobile devices, as well as technical tools, such as specialized software (EnCase, Oxygen, UFED).*

*It was established that the search of mobile terminals encompasses procedural, forensic, and technical components. The content of data stored in mobile devices was identified, including contacts, messages, geolocation, browser history, graphic files, and more. It was proven that non-compliance with procedural requirements when accessing private information may result in the data obtained being deemed inadmissible evidence. The primary investigative actions for collecting digital information were identified as temporary access to items and documents, search, inspection, and forensic examination. The tactics of conducting a search are divided into three stages: preparatory, working (including external, structural, and*

*informational inspections), and final. The study analyzed the specifics of examining smartphone content, including files, messages, browsers, and map-based applications, emphasizing the need for proper documentation of findings (via protocols, photography, and video recording). It was established that the technical component involves the use of specialized software for data analysis, recovery of deleted files, and fixation of digital traces.*

*In conclusion, the importance of adhering to procedural norms during the search of mobile terminals to ensure legality and protect personal rights was substantiated. Proposals were made to improve search tactics through clear structuring of stages and the use of modern technical tools. The findings can be utilized to enhance pre-trial investigation practices and develop recommendations for investigators and forensic experts.*

***Keywords:*** *criminal proceedings, search, inspection, temporary seizure of property, seizure of property, digital information, tactical techniques, investigation of smartphone content.*

**Постановка проблеми.** Сучасне повсякденне суспільне життя неможливо уявити без здійснення комунікацій за допомогою мобільного зв'язку. За даними дослідження інтернет-портала про інформаційні технології та інформаційну безпеку Global Report Digital, кількість користувачів мобільних пристроїв у світі у жовтні 2024 р. досягла 5,8 мільярда осіб, що становить понад 71,3 % населення планети. Число користувачів Інтернетом становить 5,35 мільярдів, тобто понад 68 % від загальної чисельності населення світу [1]. В теперішній час неможливо уявити людину, яка б не користувалася мобільним зв'язком в професійному та побутовому спілкуванні.

Поряд з очевидною користю для суспільства розвиток інформаційних технологій призвів до значного збільшення злочинів, які скоюються з використанням мобільних пристроїв. Мобільний зв'язок широко застосовується у злочинній діяльності для підготовки, в процесі вчинення

та приховання кримінальних правопорушень. Як результат протиправних дій у засобах мобільного зв'язку виникають і формуються сліди злочину як відомості, виявлення, фіксація, вилучення та дослідження яких можуть сприяти розкриттю і розслідуванню конкретних видів кримінальних правопорушень. Вказані дані утворюється як в операційно-інформаційних системах центрів комунікації оператора мобільного зв'язку, так і безпосередньо в самому мобільному терміналі, який можна розглядати як незамінне, важливе джерело криміналістично значущої інформації [2, с. 134].

Особливістю доступу до даних, які знаходиться у мобільних терміналах, є те, що значна їх частина включає приватну інформацію. Відповідно до ст. 8 «Конвенції про захист прав та основних свобод особи» кожна людина має право на повагу до її особистої та сімейної таємниць, честі, репутації, житла та листування. Слідом за міжнародно-правовими актами, український законодавець також закріпив права на таємницю кореспонденції. Згідно зі ст. 31 Конституції України «кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції» [3]. Відповідні норми, що конкретизують дані положення стосовно кримінального судочинства, закріплені, зокрема у статтях. 14, 162 КПК України (далі – КПКУ) [4].

Внаслідок появи нового виду джерел доказових відомостей – мобільних терміналів систем зв'язку, обмеженнями щодо інформації приватного характеру, у кримінальному процесуальному кодексі України внесено зміни, які регулюють права слідчого, прокурора здійснювати пошук і фіксування комп'ютерної інформації під час обшуку й огляду в тому числі в мобільних терміналах системах зв'язку [5].

Проблеми, що виникають у слідчий практиці під час обшуку та огляду мобільних терміналів систем зв'язку, викликають необхідність дослідження особливостей пошуку, аналізу цифрової інформації в цих пристроях. В зв'язку з цим автор на підставі загальних криміналістичних положень

тактики обшуку вважає за необхідне розроблення алгоритму пошуку важливої у кримінальному провадженні інформації, яка міститься в мобільних терміналах, з урахуванням особливостей етапів обшуку та виду інформаційних даних.

**Мета дослідження.** Мета статті – висвітлити правову основу, тактичні особливості проведення обшуку та огляду мобільних терміналів систем зв'язку з метою отримання криміналістично значущої цифрової інформації під час кримінального провадження.

Для досягнення цієї мети потрібно вирішити такі завдання: запропонувати порядок процесуальних дій при підготовці, проведенні та після обшуку мобільних терміналів зв'язку; розкрити тактичні особливості підготовчого, робочого та заключного етапів обшуку вмісту мобільних терміналів зв'язку; на прикладі смартфону конкретизувати види цифрової інформації (комп'ютерних даних), які потрібно встановити під час обшуку мобільних терміналів.

**Стан опрацювання проблематики.** Проблемам процесуального порядку, криміналістичних способів отримання, фіксації, вилучення та оцінки інформації під час огляду комп'ютерних засобів присвятили свої дослідження вітчизняні дослідники: В. В. Вапнярчук, А. М. Гаркуша, В. О. Голубєв, А. В. Гутник, Н. М. Дяченко, С. В. Єськов, І. Г. Каланча, М. П. Климчук, О. Г. Козицька, О. О. Кравчук, В. О. Княждвірський, А. В. Коваленко, М. В. Кобець, Н. С. Козак, С. М. Корнійко, О. Кравчук, А. І. Кунтій, О. В. Курман, Д. В. Лісніченко, Д. О. Максимус, Д. В. Пашнєв, С. В. Самойлов, А. В. Скрипник, І. А. Смаль, Б. Б. Теплицький, Є. С. Хижняк, А. Я. Хитра, Б. В. Черняховський, А. Г. Шило, М. Г. Щербаковський, В. В. Юсупов, О. О. Юхно та ін. Серед робіт доцільно виокремити монографічні дослідження. Б. В. Черняховський та В. В. Юсупов розглядали обшук приміщення, в якому знаходяться комп'ютери, під час розслідування несанкціонованого доступу до об'єктів критичної інформаційної інфраструктури [ 6 , с. 29-46]. Участь адвоката у перебігу обшуку комп'ютерної

техніці розкрито О. І. Литвинчуком, М. С. Сорокою, І. В. Колесниковим [ 7 , с. 40-53]. Особливості збирання електронних доказів у кримінальному провадженні відмічено О. О. Торбасом [ 8 , с. 119-124]. Групою авторів розроблено рекомендації щодо виявлення, огляду, фіксації, вилучення та упакування носіїв електронних (цифрових) доказів [ 9 , с. 12-45]. Способам збирання електронних доказів у кримінальному провадженні присвячено роботу А. В. Гутник та А. Я. Хитри [ 10 , с. 101-135]. В. В. Вапнярчук [11], А. М. Гаркуша, І. Г. Каланча [12] запропонували алгоритми огляду електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку під час кримінального провадження, в яких зроблено акцент на процесуальній стороні огляду, обшуку, тимчасового вилучення цих об'єктів. Водночас тактиці обшуку мобільних терміналів (телефонів) в літературі не приділено достатньої уваги.

Динамічний розвиток інформаційних технологій, розширення функціональних можливостей мобільних пристроїв вимагає необхідність постійного вдосконалення законодавства, методик збирання, дослідження та використання цифрової інформації, яка міститься в цих пристроях. Залишаються недостатньо дослідженими чимало питань щодо правових та тактичних основ обшуку та огляду мобільних пристроїв з метою отримання криміналістично значущої інформації. Крім того, тактичні прийоми проведення цих слідчих (розшукових) дій залежать від ситуацій, що характеризують обстановку місця знаходження мобільних пристроїв, їх стан, поведінку учасників. Тому вказані процесуальні дії й тактичні прийоми вимагають подальшого дослідження, що й зумовлює актуальність обраної тематики.

**Виклад основного матеріалу.** Для розв'язання завдань дослідження необхідно визначитися із термінами. Відповідно до Закону України «Про електронні комунікації» мобільний зв'язок – це «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», а кінцевим (термінальним) обладнанням

розуміються «обладнання, призначене для з'єднання з кінцевим пунктом електронної комунікаційної мережі з метою забезпечення доступу до електронних комунікаційних послуг» [13, пункти 41, 59 ст. 2]. Мобільний термінал систем зв'язку – це пристрій, який дозволяє здійснювати та підтримувати сеанси зв'язку вільно переміщаючись в межах дії мережі без підключення до іншого обладнання. Таким терміналом найчастіше є мобільний телефон (смартфон). Основні ознаки мобільного терміналу: компактність, портативність; автономне живлення від акумулятора; підтримка бездротової мережі (Wi-Fi, Bluetooth), мобільної мережі (3G/4G/5G); наявність операційної системи (Android, iOS и др.); функції зв'язку – голосові дзвінки, повідомлення, відео дзвінки та ін.

Безпосередньо в мобільному телефоні, а також на сім карті та флеш картах, які в ньому використовуються, містяться такі відомості: телефонна книга з переліком контактів; журнал вхідних, вихідних і пропущених дзвінків; вхідні та вихідні повідомлення, в тому числі, надіслані різноманітними месенджерами; звукозаписи та голосові повідомлення; фотографії, відеозаписи, графічні малюнки; календар, будильник, нагадування, списки справ; письмові тексти; повідомлення, надіслані та отримані за допомогою сервісів електронної пошти; історія відвідувань вебсайтів; документи та файли будь-якого типу; ідентифікатори користувача (наприклад, PIN); ідентифікатори приладу (IMEI); каталог використаних мереж, зокрема бездротових локальних мереж Wi-Fi; інформація про геолокацію, утворена внаслідок користування вбудованими приймачами GPS; слова, додані в базу даних системи інтелектуального введення тексту; налаштування GPRS, WAP та інтернету, цифрові гаманці (e-Wallet), а також проведені за їх допомогою фінансові онлайн-транзакції; логіни та паролі для входу в акаунти соціальних мереж; біометрична аутентифікаційна інформація (зразки відбитків пальців, роговиці ока, рис обличчя для розблокування телефону) тощо [14, с. 90].

Ефективне запобігання та протидія злочинам, для вчинення яких

використовуються інформаційні технології та мобільні термінали систем зв'язку є однією з найважливіших проблем, яку слід вирішувати процесуальними засобами й криміналістичними методами. В даний час мобільні телефони стали сховищем інформації, що є об'єктом захисту та регулювання особистих немайнових прав. Доступ до такої інформації складається з сукупності обов'язкових процесуальних вимог, недотримання яких свідчить про незаконність дій органів досудового розслідування, надмірне втручання держави у приватне життя особи та тягне за собою визнання отриманих під час огляду мобільного терміналу відомостей неприпустимим доказом.

З розвитком інформаційних технологій відбувається модернізація слідчих дій, яка проявляється не лише у можливості використовувати цифрові методи в процесі збирання чи дослідженні доказів, а й у появі нових дій, здатних додатково обмежувати права учасників судочинства, а тому потребують спеціального законодавчого регулювання. Наразі під час досудового розслідування такими слідчими (розшуковими) діями спрямованими на збирання цифрової інформації в мобільних терміналах є тимчасовий доступ до речей і документів (ст. 159 КПКУ), обшук (ст. 236 КПКУ), огляд (ст. 237 КПКУ), експертиза (ст. 242 КПКУ).

Слід зазначити, що у зарубіжному законодавстві немає єдиного порядку доступу до інформації в мобільних телефонах. У Великобританії дії, пов'язані з пошуком та вивченням даних, що зберігаються в пам'яті телефону та сім-карті, здійснюються в межах експертизи, що складається з таких етапів як: отримання мобільного телефону; вивчення смартфона з використанням інструментів цифрової криміналістики; вилучення даних, їх класифікація та аналіз; відновлення цифрових слідів [15]. Відповідно до правила 41 Федеральних правил кримінального процесу США судами видається дозвіл на обшук (виїмку) комп'ютерних засобів [16]. Специфіка обшуку, огляду мобільного терміналу як конкретного предмету, полягає в тому, що включає не тільки зовнішнє візуальне спостереження, але дослідження вмісту, аналіз, сортування відомостей, носієм яких він є.

Процедура обшуку мобільних пристроїв включає три складові: процесуальну, криміналістичну, технічну. В. В. Вапнярчук [10], А. М. Гаркуша, І. Г. Каланча [11] запропонували алгоритми огляду електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку під час кримінального провадження, в яких зроблено акцент на процесуальній стороні огляду, обшуку, тимчасового вилучення цих об'єктів. Коротко процесуальні дії мають таку послідовність (з певними виключаннями):

1) зовнішній огляд мобільного терміналу з наступним вилученням (абз. 2, 3 ч. 2 ст. 168 КПКУ), визнання тимчасово вилученим майном (ч. 2 ст. 168 КПКУ), визнанням речовим доказом (ч. 1 ст. 98 КПКУ), накладення арешту на майно (ст. 160 КПКУ), тимчасовий доступ до речей та документів (ст. 159 КПК), при необхідності – призначення експертизи (ст.242 КПКУ);

2) зовнішній огляд з наступним копіюванням цифрової інформації (абз. 4, 5 ч. 2 ст. 168 КПКУ), призначення експертизи (ст.242 КПКУ);

3) зовнішній огляд з наступним дослідженням цифрової інформації – комп'ютерних даних (абз. 1, 2 ч. 6 ст. 236 КПК, ч. 1 ст. 237 КПК).

Відповідно до положень криміналістичної тактики проведення обшуку (огляду) поділяється на три етапи: підготовчий, робочий та заключний [17, с. 51-53]. Зміст підготовчого етапу становлять визначення місця та часу проведення обшуку, підбір та запрошення учасників (понятих, спеціаліста), підготовка технічних засобів. Робочий етап – безпосередньо візуальне сприйняття та дослідження вмісту телефону. Заключний етап – складання протоколу обшуку, ознайомлення із ним учасників дії, перегляд відеозапису обшуку (у разі, якщо така проводилася).

На робочому етапі можна виділити три стадії огляду мобільного терміналу:

1) зовнішній огляд, що включає фіксацію відомостей про зовнішню будову та стан мобільного термінала, а також його специфічні прикмети;

2) конструктивний огляд, під час якого провадиться вивчення складових частин телефону;

3) огляд інформаційної складової, що передбачає вивчення відомостей, які зберігаються в пам'яті телефону, на флеш- та Sim-картах.

Технічна складова обшуку, наприклад сматрфонів, передбачає використання спеціалізованого програмного забезпечення. Прикладами таких прикладних програм є EnCase, Encase, DFF, Helix, Oxygen, MOBILEdit и UFED, Smartphone Examiner, Mobile Phone Examiner Plus та ін. [18, 19]. Ці інструменти, розроблені для співробітників підрозділів кіберполіції та фахівців з інформаційної безпеки, з метою збирання доказів з мобільних пристроїв, дозволяють фізично отримувати логічні дані з пристроїв, створювати образи систем, які підтримують. Після проведення обшуку мобільного пристрою можливе копіювання встановленої інформації спеціалізованою програмою FTK (Forensic Toolkit) для подальшого дослідження, наприклад, відновлення віддалених файлів [20]. Британською асоціацією керівників поліцейських служб (ACPO) розроблено спеціальну інструкцію з вилучення доказів з мобільних пристроїв [21]. Фахівці відмічають, що процедура вилучення даних з мобільних пристроїв відрізняється від вилучення інформації з персональних комп'ютерів з огляду на те, що мобільні пристрої, порівняно з персональними комп'ютерами, мають більш вузькі завдання, архітектуру процесора, операційну систему і т. д. У зв'язку з цим методи та особливості проведення процесуальних дій повинні бути індивідуальними [22, с. 69.]

Огляд апаратного забезпечення включає встановлення IMEI – унікального числа для кожного апарату, яке присвоюється мобільному пристрою в процесі виготовлення на заводі. IMEI можна знайти у вигляді напису всередині пристрою або за допомогою набору наступних символів на клавіатурі «*#06#». Цифрові сліди, що містяться в мобільному терміналі, найчастіше знаходяться в пам'яті телефону, в графічних файлах, крос-платформній системі миттєвого обміну повідомленнями Telegram, Viber, WhatsApp; в програмах для пошуку та перегляду інформації з мережі Інтернет – браузерах Internet Explorer, Google, Safari, Chrome та ін.; додатках, побудованих на основі картографічних сервісах Google Maps, Waze тощо.

*Аналіз файлів.* Графічні файли розташовуються в пам'яті мобільного пристрою у вигляді знімків екрана, фотографій, завантажених зображень і т. д. У цих файлах може міститися інформація про час та місце зйомки. Особливу увагу під час огляду мобільного пристрою необхідно приділити віддаленим графічним файлам, які містяться у спеціальних альбомах обмежений час (зазвичай 30 днів). У різних моделях мобільних терміналів ці альбоми мають різну назву, наприклад «нещодавно видалені», «кошик» й т.п. Для збереження графічних файлів у пам'яті телефону необхідно відновити їх із зазначених альбомів шляхом вибору дії «відновити», «відновити всі». Маніпуляції в телефоні та кількість відновлених фотографій необхідно відобразити у протоколі, зображення фіксувати за допомогою фотозйомки екрана мобільного термінала, а також можна використовувати відеозйомку для фіксації дій слідчого (спеціаліста).

При описі певного виклику в телефоні вказується його вид (вхідний, вихідний, не прийнятий), час, тривалість, дані абонента, з яким здійснено контакт, а також його абонентський номер. Останнє особливо важливе для встановлення інших співучасників злочину, потерпілих, які не зверталися до поліції за фактом скоєного стосовно них злочину. Опис SMS-, MMS-повідомленнь включає відповідно їх текстовий та (або) графічний вміст (тип, розмір, час створення файлу, хто зображений, тривалість ролика).

*Аналіз повідомлень.* Встановлюється абонентський номер користувача пристрою. Абонентські номери інших осіб, нещодавні дзвінки та повідомлення, здійснені всередині системи між абонентами, можна дізнатися шляхом огляду акаунтів з абонентськими номерами, які збереглися у користувача мобільного пристрою, зареєстрованого в месенджерах Telegram, WhatsApp, Telegram, Facebook, Messenger. Найчастіше проводиться огляд особистих листувань у пам'яті пристрою без окремого судового рішення.

Під час вивчення змісту листування, яке може розташовуватися в чатах месенджерів, між абонентами (членами злочинної групи), так і в спеціально створеній групі також можуть бути виявлені текстові документи, відеофайли та графічні файли, що відображають окремі етапи злочинної діяльності. При

відкритті кожного чату, розташованого месенджерах, можна отримати доступ до графічних та відеофайлів, які будь-коли були надіслані учасникам цього чату, а також отримати іншу криміналістично значиму інформацію. Зазначені файли описуються у протоколі слідчої дії та за потреби фіксуються з використанням фотозйомки. Слід зазначити, що активне використання Telegram у протиправній діяльності злочинних груп, скоєних з використанням мережі Інтернет, зумовлене вбудованою функцією «Архівні чати», які неможливо виявити при звичайному огляді всіх наявних листувань. Такі каталоги можна знайти шляхом перегортання вниз списку всіх повідомлень, розміщених у програмі Telegram.

*Аналіз програм для пошуку та перегляду інформації з мережі Інтернет* – браузерів Google Chrome, Safari, Opera, Telegram та ін., що встановлені на смартфонах. Криміналістично значущу інформацію в рамках розслідування кримінальних правопорушень, скоєних з використанням мережі Інтернет, можна отримати при ознайомленні з історією перегляду веб-сторінок та закладок зазначених браузерів (форуми, на яких члени злочинної групи могли спілкуватися між собою і потерпілими, відомості про заборонені до обігу предмети – наркотики, вибухові речовини та ін.). При переході на вкладці «Історія» в веб-браузері Safari на екрані мобільного пристрою з’явиться інформація про всі веб-сторінки з адресами електронних ресурсів (URL-адреси), на які власник телефону здійснював перехід. Зазначені сторінки розташовуються за датою відвідування користувачем останньої веб-сторінки (найвища в рядку) до першої. В деяких моделях пристроїв перелік браузерів можна оглянути також шляхом переходу на вкладки «Закладки» через вкладку «Налаштування». У закладках відображаються URL-адреси всіх веб-сторінок, збережених користувачем спеціально. URL-адреси веб-сторінок, які знаходяться в історії перегляду та закладках браузерів, повинні бути зафіксовані в протоколі слідчого огляду предмета. Надалі зазначені адреси мають бути оглянуті слідчим з використанням персонального комп'ютера з виходом до мережі Інтернет під час проведення огляду комп’ютерних даних (ст. 237 КПК України).

*Аналіз застосунків, побудованих з урахуванням картографічних сервісів.* В

історії пошуку даних сервісів можуть відображатись різні місця з адресами, які вводилися туди користувачем телефону. Наприклад, доступ до історії пошуку у сервісі Google maps можна отримати шляхом одноразового натискання на рядок пошуку. В результаті цього можуть бути виявлені різні адреси від останньої введеної адреси користувачем (найвищий у рядку) до самого першого. У Waze навігаторі історія адрес пошуку відображається на екрані відразу після відкриття сервісу. Дані адреси можуть виступати як місцем скоєння злочинів, так і свідчити про знаходження власника мобільного пристрою в певному місці в певний час. Виявлені адреси підлягають фіксації в протоколі в послідовності, що відобразилася.

У разі виявлення графічних файлів, які мають криміналістично значущу інформацію, необхідно описати зазначені файли у протоколі огляду смартфона. Крім того, ці файли можуть бути зафіксовані за допомогою фотозйомки екрана мобільного пристрою, після чого можна скопіювати файли за допомогою підключення телефону до персонального комп'ютера через USB-порт. Скопійовані файли записуються на дисковий носій, який додається до протоколу обшуку.

Судова практика свідчить, що сторона захисту часто заперечує встановлені без ухвали слідчого судді файли та повідомлення. У судових інстанціях в одних випадках суди підтримували правозастосовників, в інших визнавали протоколи таких оглядів недопустимими доказами у кримінальному провадженні. На нашу думку, для запобігання клопотанням сторони захисту про недопустимість виявленої інформації як доказу, слід або заздалегідь отримати рішення слідчого судді про дозвіл на обшук (огляд) або звернутися за ним одразу після проведення невідкладного обшуку (огляду) – ч. 5 ст. 171 КПКУ.

**Висновки.** Розвиток інформаційних технологій призвів до значного збільшення злочинів, які скоюються з використанням мобільних пристроїв. В результаті протиправних дій у засобах мобільного зв'язку виникають і формуються сліди злочину, які є важливими джерелами криміналістично значущої інформації й можуть бути виявлені під час огляду, обшуку,

тимчасового доступу. Процедура обшуку мобільних терміналів включає три складові: процесуальну, криміналістичну, технічну. Оскільки дані, що містяться в терміналах, включають приватну інформацію, це вимагає особливого процесуального режиму до їх доступу. Доступ до такої інформації складається з сукупності обов'язкових процесуальних вимог, недотримання яких веде до визнання отриманих під час огляду мобільного терміналу відомостей неприпустимим доказом. Під час досудового розслідування слідчими (розшуковими) діями, які спрямовано на збирання цифрової інформації в мобільних терміналах, є тимчасовий доступ до речей і документів, обшук, огляд, експертиза.

Тактика обшуку поділяється на три етапи: підготовчий, робочий та заключний. Робочий етап включає три стадії: зовнішній огляд, що спрямований на фіксацію відомостей про зовнішню будову та стан мобільного термінала, а також його специфічні прикмети; конструктивний огляд, під час якого провадиться вивчення складових частин телефону; огляд інформаційної складової, що передбачає вивчення відомостей, які зберігаються в пам'яті телефону, на флеш- та Sim-картах. Технічна складова обшуку передбачає використання спеціалізованого обладнання та програмного забезпечення. Дослідження вмісту смартфонів включає: аналіз файлів, повідомлень, програм для пошуку та перегляду інформації з мережі Інтернет, застосунків, побудованих з урахуванням картографічних сервісів. Фіксація виявленої інформації здійснюється описом в протоколі, за допомогою фотозйомки, відео фіксації екрана та дій слідчого (спеціаліста).

## Список використаних джерел

1. Digital 2024 october Global Statshot Report. URL: https://wearesocial.com/uk/blog/2024/10/digital-2024-october-global-statshot-report/ (дата звернення: 10.07.2025).

2. Козицька О. Засоби рухомого (мобільного) зв'язку як джерело криміналістично значущої інформації. *Університетські наукові записки*. 2020, № 5 (77). С. 132-141.

3. Конституція України: Закон України від 26 червня 1996 р. *Відомості Верховної Ради України* (ВВР), 1996, № 30, ст. 141. URL:https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text (дата звернення: 10.07.2025).

4. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 року № 4651-VI. *Відомості Верховної Ради України* (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 10.07.2025).

5. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами та протидії кібератакам: Закон України № 2137-IX від 15 березня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 10.07.2025).

6. Черняховський Б. В., Юсупов В. В. Проведення обшуку під час розслідування несанкціонованого доступу до об'єктів критичної інформаційної інфраструктури: методичні рекомендації. Київ : Нац. акад. внутр. справ, 2021. 52 с.

7. Електронні докази. Обшук. Частина 1 / О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін. Харків : Фастор, 2020. 80 с.

8. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса: Вид. «Юридика», 2024. 180 с.

9. Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації / М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

10. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи вико- ристання електронних документів у доказуванні: колективна монографія. Львів : ЛьвДУВС, 2022. 204 с.

11. Вапнярчук В. В. Щодо дослідження змісту електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку під час кримінального провадження. Аналітично-порівняльне правознавство. 2025. Вип. 2. С. 967-972

12. Гаркуша А. М., Каланча І. Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи* : матеріали круглого столу (м. Львів, 11 червня 2021 р.) Львів : Львівський державний університет внутрішніх справ, 2021. С. 159–165

13. Про електронні комунікації : Закон України від 16 грудня 2020 року № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 10.07.2025).

14. Androulidakis I. I. Mobile Phone Security and Forensics: A Practical Approach. Second Edition. Switzerland : Springer International Publishing, 2016. 120 p.

15. Tajuddin T. B., Manaf A. A. Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone. 2015 *World Congress on Internet Security* (*WorldCIS*), Dublin, 19-21 October 2015, 132-138. URL: https://doi.org/10.1109/WorldCIS.2015.7359429 (дата звернення: 10.07.2025).

16. Rule 41. Search and Seizure. Federal Rules of Criminal Procedure. URL:https://www.law.cornell.edu/rules/frcrmp/rule_41 (дата звернення: 10.07.2025).

17. Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : посібник. Харків: Харк. нац. ун-т внутр. справ, 2010. 112 с.

18. Kumar R., Mohana P., Reddy P. N., Varshini N. A Forensics Activity Logger To Extract User Activity From Mobile Devices. *Turkish Journal of Computer and Mathematics Education.* 2024. Vol. 15. No. 3. P. 205-217.

URL:https://ru.scribd.com/document/849648905/a-forensics-activity-logger-to-extract-user-activi (дата звернення: 10.07.2025).

19. Щербаковський М., Сезонов В. Збирання та дослідження електронних документів із застосуванням спеціальних знань. *Теорія та практика судової експертизи та криміналістики.* 2024. Вип. 3 (36). С. 11–23.

20. AD Forensic Tool Kit (FTK) URL: https://cybermarket.com.ua/product/ad-forensic-tool-kit-ftk/ (дата звернення: 10.07.2025).

21. ACPO. Managers Guide. Good Practice and Advice Guide for Managers of e-Crime Investigation. URL:https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_and_Advice_for_Manager_of_e-Crime-Investigation.pdf (дата звернення: 10.07.2025).

22. Sammons J., Brunty J. Mobile device forensics: threats, challenges and future trends. *Digital Forensics: Threatscape and Best Practices.* Syngress, 2015, 182 p.