Установлення особи, підозрюваної у скоєнні кіберзлочину з використанням *WiFi*-технологій

Юрій Нізовцев * [a], Олег Парфило ** [b], Олег Плахотнік * [c]**

* Канд. юрид. наук, Український науково-дослідний інститут спеціальної техніки та судових експертиз СБУ, м. Київ, Україна, ORCID: https://orcid.org/0000-0002-7641-6403, e-mail: nizovtsev.yurii@gmail.com
** Канд. юрид. наук, Український науково-дослідний інститут спеціальної техніки та судових експертиз СБУ, м. Київ, Україна, ORCID: https://orcid.org/0000-0001-8787-7478, e-mail: parfylo.oleg@gmail.com
*** Канд. юрид. наук, доц., Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка, м. Київ, Україна, ORCID: https://orcid.org/0000-0002-2787-6956, e-mail: knukyiv1@gmail.com

[a] Написання оригінального рукопису, методологія, формальний аналіз.
[b] Написання оригінального рукопису, адміністрування проєкту, методологія, нагляд.
[c] Написання оригінального рукопису, методологія, формальний аналіз, ресурси (джерела).

DOI: 10.32353/khrife.4.2023.03 УДК 343.98:004.7
Надійшло 20.11.2023 / Рецензовано 22.11.2023 / Прийнято до друку 18.12.2023 / Доступно онлайн 29.12.2023

Мета статті — дослідити питання використання WiFi-маршрутизаторів та інформації, яку вони містять, під час розслідування кіберзлочинів, учинених із використанням WiFi-технології, як методу, ефективного для встановлення підозрюваної особи або групи осіб з подальшим визначенням місця їх знаходження. Для досягнення поставленої мети застосовано загальнонаукові та спеціальні наукові методи дослідження. Опрацьовано різні методичні рекомендації щодо використання WiFi-маршрутизаторів для встановлення мобільного пристрою шляхом судово-експертного дослідження. Наголошено, що в разі скоєння кіберзлочину із застосуванням WiFi-маршрутизатора, спеціаліст та експерт можуть використати технічну інформацію з WiFi-маршрутизатора для ідентифікації мобільного пристрою підозрюваної особи за MAC-адресою. Розглянуто проблемні питання із виявлення ознак приховування цифрових слідів під час скоєння кіберзлочину. Викладено процесуальний порядок отримання доступу

до WiFi-маршрутизаторів із метою встановлення підозрюваної особи під час огляду, обшуку й розслідування кіберзлочинів. Доведено, що дані з WiFi-маршрутизаторів сприятимуть не тільки встановленню підозрюваних осіб у кримінальних провадженнях під час розслідування кіберзлочинів: цей метод може виявитися універсальним для встановлення підозрюваних осіб у кримінальних провадженнях із неповними даними. Проаналізовано термін «комп'ютерні дані», відзначено особливу роль спеціаліста у проведенні огляду комп'ютерних даних і запропоновано змінити чинний Кримінальний процесуальний кодекс України в частині участі спеціаліста в огляді комп'ютерних даних за дорученням слідчого, прокурора й дізнавача під час досудового розслідування кримінальних проступків. Положення та висновки авторського дослідження стануть у пригоді в оперативно-розшуковій, слідчій і судово-експертній діяльності.

Ключові слова: *кіберзлочини; маршрутизатори; WiFi-технології; електронні комунікації; електронні докази; цифрові сліди; розслідування; судова експертиза; методичні рекомендації.*

Постановка наукової проблеми

Використання *WiFi*-маршрутизаторів та інформації, яку вони містять, під час розслідування кіберзлочинів може бути надзвичайно ефективним методом для сторони обвинувачення у процесі встановлення місця знаходження підозрюваної особи й використання технічної інформації з таких маршрутизаторів як електронних доказів, що зберегли цифрові сліди [1] скоєння кіберзлочину. *WiFi*-маршрутизатори — це пристрої, призначені для безпровідного з'єднання мобільних абонентських терміналів з інтернетом та іншими мережевими ресурсами. Функційно вони маршрутизують (спрямовують у певному напрямку) пакети інформації між бездротовими пристроями й інтернетом. У процесі комунікації відбувається передавання як інформації користувача (трафік команд віддаленого керування, уміст вебсторінки сайту, скачування певного файлу, передавання відеопотоку тощо), так і службових даних, необхідних для функціювання мережі. Службові дані, поміж іншим, містять інформацію про мобільний пристрій, а користувацька інформація характеризує мережеву активність і може містити цифрові сліди кібератаки або інших незаконних дій. До того ж *WiFi*-маршрутизатор може містити певну інформацію про службові дані та мережеву активність — так звані логи. Отже, після скоєння підозрюваною особою кіберзлочину з використанням *WiFi*-маршрутизатора спеціаліст та експерт можуть застосувати технічну інформацію з *WiFi*-маршрутизатора для

1 Омельян О. С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 461. DOI: 10.33994/kndise.2020.65.45 (дата звернення: 17.10.2023).

ідентифікації мобільного пристрою підозрюваної особи за *MAC*-адресою. Цю інформацію сторона обвинувачення також може використати для деанонімізації та з'ясування місця знаходження підозрюваної особи або групи осіб і справжнього місця їх виходу в мережу за такими фактичними даними. Застосовуючи цей метод, необхідно дотримувати відповідних процесуальних процедур щодо отримання інформації з *WiFi*-маршрутизатора та її належного збереження з метою подальшого використання стороною обвинувачення такої інформації як доказів у кримінальному провадженні.

Із позицій процесуальності питання електронних доказів [2] у кримінальному провадженні потрібно врегулювати на законодавчому рівні: законодавство має містити порядок отримання доступу до *WiFi*-маршрутизаторів із метою встановлення підозрюваної особи під час огляду, обшуку, розслідування кіберзлочинів і виконання інших завдань кримінального провадження. Отримання ж доступу до *WiFi*-маршрутизатора в необумовлений законом спосіб може спричинити порушення прав людини, а за Конвенцією про захист прав людини і основоположних свобод *«кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції»* (ч. 1 ст. 8) [3]. Оскільки *WiFi*-маршрутизатори здатні зберігати інформацію про пристрої, які підключаються до них, включно з *MAC*-адресами пристроїв, *IP*-адресами, часом підключення, інформацією про вебсайти тощо, то цю інформацію сторона обвинувачення може використати для встановлення підозрюваної особи, відстеження переміщень такої особи та її активності в інтернеті на момент скоєння кіберзлочину. Тому можна стверджувати, що процесуальний аспект розслідування кіберзлочинів повинен містити зрозумілий порядок дій спеціалістів і експертів у спільній роботі з органами досудового розслідування та процесуальним керівником для отримання доказів обвинувачення у кримінальному провадженні. Окрім того, дані з *WiFi*-маршрутизаторів можна використати не тільки для встановлення підозрюваних осіб у кримінальних провадженнях під час розслідування кіберзлочинів: цей метод може виявитися універсальним для визначення підозрюваних осіб у кримінальних провадженнях із неповними даними.

2 Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. Вип. 14. С. 208—214. DOI: 10.33244/2521-1196.14.2019.208-214 (дата звернення: 17.10.2023) ; Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3—2. С. 316—318. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf (дата звернення: 17.10.2023) ; Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247—253. URL: http://nvppp.in.ua/vip/2018/2/50.pdf (дата звернення: 17.10.2023) ; Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Вид. 2-ге, допов. Київ, 2020. 104 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content (дата звернення: 17.10.2023).

3 Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) : від 04.11.1950 р.; ратифік. Законом України від 17.07.1997 р. № 475/97-ВР; чинна для України з 11.09.1997 р. (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 17.10.2023).

Мета статті

Розглянути актуальні проблеми, пов'язані з ідентифікацією підозрюваних осіб у скоєнні кіберзлочинів, зокрема тих, які використовують технологію *WiFi*. Дослідити можливість установлення осіб, підозрюваних у скоєнні кіберзлочинів, які активно приховують цифрові сліди своєї діяльності. Проаналізувати термін «комп'ютерні дані», а також роль та участь спеціаліста в такій процесуальній дії, як огляд у контексті розслідування кіберзлочинів.

Методи дослідження

Для досягнення поставленої мети застосовано загальнонаукові (діалектичний, порівняння, аналіз, синтез, індукцію, дедукцію) і спеціальні наукові методи (формально-логічний, логіко-юридичний, системно-структурний), що сприяло змістовності й обґрунтованості наукових висновків і пропозицій цього дослідження.

Аналіз основних досліджень і публікацій

На науковому рівні питання використання *WiFi*-роутерів та інформації, яку вони містять, у кримінальному провадженні не лише привернуло увагу, а й стало об'єктом глибокого аналізу провідних учених та експертів. Багато науковців і практиків присвятили свої час і зусилля дослідженню цього складного питання (зокрема, у таких наукових галузях, як криміналістика та судова експертологія). Із-поміж останніх дослідницьких робіт і методичних рекомендацій, присвячених використанню *WiFi* та сучасних мобільних технологій для ідентифікації осіб, підозрюваних у скоєнні кримінальних правопорушень, можна виокремити кілька надзвичайно цікавих і перспективних праць.

Наприклад, М. Кобець і Р. Кобець у 2022 році розглянули дії слідчо-оперативної групи в контексті ідентифікації особи, яка скоїла кримінальне правопорушення, за наявності на місці події *WiFi*-роутера (комп'ютерної техніки, яка потребує спеціальних знань) [4], запропонували застосовувати скриншот до концепції електронних доказів у кримінальному провадженні, навели науково-методичні рекомендації, які можна використовувати для встановлення особи, що вчинила кримінальне правопорушення. 2023 року М. Кобець дослідив 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* (згадана публікація заслуговує на увагу в контексті логіки розвитку подій для встановлення підозрюваної особи у кримінальному провадженні) [5].

В. Поливода 2021 року проаналізував проблематику встановлення за допомогою *WiFi* осіб, причетних до скоєння

4 Кобець М. В., Кобець Р. М. Використання можливостей Wi-Fi роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник*. 2022. № 2 (38). С. 36—47. DOI: 10.37025/1992-4437/2022-38-2-36 (дата звернення: 17.10.2023).

5 Кобець М. В. Дії слідчого під час виявлення на місці події мобільних терміналів (стільникових радіотелефонів). *Там само*. 2023. № 1 (39). С. 52—63. DOI: 10.37025/1992-4437/2023-39-1-52 (дата звернення: 17.10.2023).

злочинів, і навів приклади із досвіду іноземних колег [6].

У науково-методичних рекомендаціях для підрозділів Національної поліції України «Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів» (2022) частково розкрито питання використання *WiFi* для пошуку осіб, причетних до незаконного обігу наркотичних засобів за допомогою інтернету: *«У сприятливих умовах встановити таких осіб можна, наприклад, за результатами перегляду записів камер відеоспостереження, які встановлено у приміщеннях, де використовувались певні зони Wi-Fi-зв'язку, де збувальник наркотиків виходив у мережу "Інтернет"»* [7]. Незважаючи на те, що ці рекомендації не спрямовані на предметне розслідування кіберзлочинів, їхній логічний зв'язок із методикою встановлення підозрюваної особи з використанням *WiFi* є очевидним: вони можуть стати в пригоді під час розслідування кіберзлочинів, хоча й не передбачають досліджень конкретних випадків подібних правопорушень.

На нашу думку, варто відзначити надзвичайно перспективні та якісні методрекомендації «Використання можливостей *Wi-Fi* маршрутизаторів для встановлення мобільного терміналу та його мережевої активності», підготовлені 2022 року в Українському науково-дослідному інституті спеціальної техніки та судових експертиз Служби безпеки України (далі — *ІСТЕ СБУ*), де висвітлено теоретичні та практичні аспекти використання *WiFi*-маршрутизатора, до якого підозрювана особа під'єднувала мобільний термінал (це допомагає визначити пристрій і місце його знаходження, а також мережеву активність, що може свідчити про кібератаку) [8]. Згадане видання призначене для співробітників експертних підрозділів, спеціалістів, оперативних працівників і слідчих.

На увагу також заслуговують методрекомендації Б. Черняховського та В. Юсупова «Проведення обшуку під час розслідування несанкціонованого доступу до об'єктів критичної інформаційної інфраструктури» (2021) [9], адже стадія загального огляду робочого етапу пошуку цього видання заслуговує на особливу увагу, а «*першочергова перевірка місць розташування об'єктів пошуку, включаючи визначення типу підключення —*

6 Поливода В. В. Можливості Wi-Fi маршрутизатора у встановленні особи, причетної до вчинення злочину. *Використання досягнень сучасної науки й техніки в розкритті злочинів* : мат-ли міжвідом. наук-практ. кругл. столу (Київ, 25.02.2021). 2021. С. 102—105 / Електронний репозитарій НАВС. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/2f7d687f-7477-4670-80f6-b73c221681dd/content (дата звернення: 17.10.2023).

7 Кікінчук В. В., Матюшкова Т. П., Піддубна А. В., Манжай О. В., Носов В. В. Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів : наук.-метод. рек. для підрозд. Нацполіції Укр. Харків, 2022. 69 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/59910657-34ae-431c-966d-eeaffcb057c8/content (дата звернення: 17.10.2023).

8 Нізовцев Ю. Ю. Використання можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності : метод. рек. Київ, 2022. 18 с.

9 Черняховський Б. В., Юсупов В. В. Проведення обшуку під час розслідування несанкціонованого доступу до об'єктів критичної інформаційної інфраструктури : метод. рек. Київ, 2021. 52 с.

кабельного чи WiFi» відповідає предмету дослідження нашої статті. Загалом ці методичні рекомендації характеризують об'єкти критичної інформаційної інфраструктури й види злочинних посягань на них шляхом несанкціонованого доступу, аналізують підстави та процесуальний порядок проведення обшуку й містять криміналістичні рекомендації щодо його проведення під час розслідування таких злочинів і порядок здійснення слідчих дій.

Окремо варто згадати монографію О. Самойленко «Основи методики розслідування злочинів, вчинених у кіберпросторі» (2020), розділи якої присвячено криміналістичній характеристиці й організації розслідування злочинів, скоєних у кіберпросторі [10].

Серед іноземних розробок зацікавленість викликає спільна праця китайських і американських науковців 2012 року, у якій запропоновано класифікувати мережеві криміналістичні розслідування за трьома категоріями (залежно від того, коли правоохоронні органи проводять розслідування у відповідь на інциденти кіберзлочинності) [11]: зокрема, проактивні розслідування визначено такими, що відбуваються до інцидентів кіберзлочинності; реальні розслідування — такими, що відбуваються під час цих інцидентів, ретроспективні розслідування — такими, що відбуваються після цих інцидентів. Як приклад пропонується застосування портативного пристрою на базі смартфону для реального визначення розташування підозрюваного, який вчинює злочини у кіберпросторі. У цьому дослідженні йдеться про збір даних, про силу бездротового сигналу *GSM* і *WiFi* та точність позиціонування за допомогою експериментів.

Окрім цього, на нашу думку, цікавими є наукові праці А. Коваленка 2017 та 2023 років [12] і Є. Хижняка 2017 року [13], у яких досліджено особливості огляду комп'ютерних даних та електронних документів під час розслідування кримінальних правопорушень. Автори наголошують, що в межах підготовки до проведення огляду комп'ютерних даних доцільно попередньо з'ясувати, із якими пристроями й типами даних доведеться працювати, забезпечити участь спеціалістів і наявність необхідних технічних засобів.

Зважаючи на активність наукових досліджень у галузі криміналістики за цифровими слідами й електронними доказами, а також на наявні методрекомендації

10 Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса, 2020. 372 с. DOI: 10.32837/11300.13264 (дата звернення: 17.10.2023).

11 Huang J., Chen Yi., Ling Zh., Choo K., Fu X. A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation / UMASS Lowell. #1 Public in mass. Massachusetts Lowell, USA, 2012. 33 p. URL: https://www.uml.edu/docs/HaLo_2012_Fu_tcm18-152079.pdf (дата звернення: 17.10.2023).

12 Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України*. 2017. № 1 (88). С. 182—191. URL: http://nbuv.gov.ua/UJRN/vapny_2017_1_19 (дата звернення: 17.10.2023) ; Його ж. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки.* 2023. Вип. 4. С. 53—58. DOI: 10.32999/ksu2307-8049/2023-4-9 (дата звернення: 17.10.2023).

13 Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право*. 2017. № 4 (58). С. 80—85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (дата звернення: 17.10.2023).

із використання *WiFi*-маршрутизаторів для цілей і завдань кримінального провадження, можна упевнено стверджувати, що тема ідентифікації підозрюваних через *WiFi*-маршрутизатори в розслідуванні кримінальних правопорушень і розшуку підозрюваних осіб залишається надзвичайно актуальною. Особливо це стосується використання зловмисниками сучасних технологій для скоєння злочинів у кіберпросторі. Саме тому використання даних із *WiFi*-маршрутизаторів для ідентифікації підозрюваних осіб набуває особливого значення на стадії досудового слідства під час розслідування злочинів за розд. XVI (ст. 361—363[1]) Кримінального кодексу України [14]. Важливо зазначити, що успішність такого методу ідентифікації підозрюваних може мати велике значення для доведення вини у кримінальному провадженні не тільки під час розслідування кіберзлочинів. Так, можна стверджувати, що головною метою використання можливостей *WiFi*-маршрутизаторів для ідентифікації підозрюваної особи з подальшим визначенням місця знаходження радіообладнання (радіоелектронного засобу) є не лише встановлення місця знаходження підозрюваної особи, а й використання цих даних як доказів обвинувачення на стадії досудового розслідування та судового провадження.

Наукова новизна полягає у пропозиції доповнити ч. 2 ст. 71 і ч. 7 ст. 237 Кримінального процесуального кодексу України [15] (далі — *КПК України*) інформацією про участь в огляді комп'ютерних даних (за дорученням слідчого, прокурора й дізнавача під час досудового розслідування кримінальних проступків) спеціаліста, який має спеціалізовані знання та розуміє процес отримання комп'ютерних даних, що містять інформацію про *MAC*-адреси з *WiFi*-маршрутизаторів. Окрім того, він має належне обладнання, яке дає змогу отримувати цифрові сліди кіберзлочину без втрати або пошкодження. На підставі аналізу наукових статей і нормативної літератури можна дійти висновку, що станом на сьогодні відсутнє чітке визначення терміна «комп'ютерні дані». Ми пропонуємо розширену інтерпретацію поняття «комп'ютерні дані», включно з інформацією, яку містять *WiFi*-маршрутизатори. Науковою новизною також можна вважати методику пошуку підозрюваних осіб, уперше запропоновану Ю. Нізовцевим, яку ми розглядаємо на науковому рівні.

Викладення основного матеріалу дослідження

У ст. 84 КПК України зазначено:

«1. Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

2. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів» [16].

Дані з *WiFi*-маршрутизаторів можуть бути одним із джерел доказів. Якщо підозрювана особа використовувала *WiFi*-мережу під час скоєння злочину, дані про її підключення до цієї мережі можна використати для її ідентифікації

14 Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 17.10.2023).

15 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.10.2023).

16 Там само.

та подальшого встановлення місця знаходження. Під даними слід розуміти *MAC*-адресу мобільного пристрою та інші технічні дані, які спеціаліст або експерт може отримати під час огляду (обшуку), що передбачає прямий доступу до маршрутизатора. Такі дані також можна використати для з'ясування зв'язків з іншими особами у межах підключень до цієї мережі. Зважаючи на наявний спосіб визначення підозрюваних осіб, що передбачає використання даних про підключення мобільного пристрою до *WiFi*-маршрутизаторів, необхідно розглянути проблемні питання, які містять можливу зміну даних про підключений мобільний пристрій із метою його приховування. Одним із проблемних питань у розслідуванні кіберзлочину є приховування інформації під час його скоєння. Таке приховування відбувається за допомогою заміни або клонування *MAC*-адреси мобільного пристрою штатними програмними засобами цього пристрою. *MAC*-адреса (від англ. *Media Access Control* — управління доступом до середовища) — це унікальний ідентифікатор мережевого інтерфейсу. У мережевій моделі *OSI* (від англ. *The Open Systems Interconnection model*) *MAC*-адресу використовують на другому (канальному) рівні. Іноді цю адресу ще називають апаратною або фізичною (англ. *Hardware Address*). *MAC*-адресу мережевому інтерфейсу надає завод-виробник, водночас адресний простір розподілено між виробниками. Зміна *MAC*-адреси може зробити умовно неможливою ідентифікацію мобільного пристрою за даними про його підключення до *WiFi*-маршрутизаторів. Іншим проблемним питанням є можливість використання *VPN*. *VPN*-з'єднання створює зашифрований канал між мобільним пристроєм і сервером *VPN*, що дає змогу приховати дані про мережеву активність мобільного пристрою, підключеного до *WiFi*-мережі, але без приховання даних про *MAC*-адресу. Тому можливість ідентифікувати мобільний термінал залишається (якщо *MAC*-адреси не змінили), хоча ознаки кібератаки (тип атаки, її ціль тощо) можуть бути приховані. Іще одним проблемним питанням є можливість використання спеціальних програмних засобів для маскування мобільного пристрою під інший пристрій, тобто навмисна зміна *MAC*-адреси не на довільну адресу, а на адресу іншого конкретного мобільного пристрою з метою його компрометації. Ці проблемні питання можуть ускладнити або унеможливити застосування наявного способу ідентифікації підозрюваних осіб, тож потребують негайного розв'язання.

У згаданих вище методрекомендаціях «Використання можливостей *Wi-Fi* маршрутизаторів для встановлення мобільного терміналу та його мережевої активності», розроблених в ІСТЕ СБУ, зазначено, що «*використання зафіксованої WiFi-маршрутизатором інформації про підключені мобільні термінали можливе у випадку, якщо маршрутизатор підтримує логіювання мережевих з'єднань і якщо таке логіювання активоване*» [17]. Тобто інформація, що характеризує безпосередньо під'єднані до *WiFi*-мережі мобільні термінали, зазвичай містить дані про мережеву назву такого термінала, його *MAC*-адресу, *IP*-адресу, час підключення до мережі та тривалість сеансу. Використовуючи довідкові дані, за *MAC*-адресою зазвичай можна визначити виробника мобільного термінала, а в окремих випадках — конкретну модель. У цих методрекомендаціях також порушено проблемні питання ідентифікації підозрюваних осіб: «*Слід враховувати*

17 Нізовцев Ю. Ю. Зазнач. твір.

певні особливості MAC-адреси. По-перше, цю адресу можна змінити у налаштуваннях мобільного термінала або використовуючи спеціальне програмне забезпечення. Наприклад, сучасні смартфони мають функцію генерації випадкової MAC-адреси при кожному підключенні до мережі <…>. По-друге, MAC-адреса не передається разом з мережевим трафіком глобально. В рамках WiFi-мережі MAC-адреса передається від термінала лише до маршрутизатора, не далі. А отже, відслідкувати у глобальній мережі мобільний термінал за його MAC-адресою зазвичай неможливо» [18].

В. Поливода у згаданій вище праці також зазначає, що «*для використання можливостей WiFi-маршрутизатора необхідно розуміти, що на самому технічному пристрої можна змінювати MAC-адресу. Її зміна відбувається тільки в тому випадку, якщо в даний момент смартфон не підключений до будь-якої WiFi-мережі. За допомогою спеціальних алгоритмів його можна виявити і відфільтрувати на пристрої з 100 % вірогідністю. Зокрема, крім випадкової MAC-адреси смартфони періодично відправляють і правильний MAC-адрес, який і отримує WiFi-радар*». Науковець також зауважує, що «*частка смартфонів, які можуть підміняти свою MAC-адресу, не більше 30 % у великих містах*» [19].

М. Кобець і Р. Кобець зазначали, що «*слідчий (оперативний працівник) на підставі ухвали слідчого судді суду першої інстанції направляє запит до мережевих операторів стільникового радіозв'язку з метою перевірки MAC-адрес, встановлених під час огляду місця події, і встановлення даних користувача (IMEI, номера телефону та інші дані), які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку*» [20]. Застосуванню цього алгоритму передусім перешкоджає те, що оператори стільникового зв'язку не мають інформації про *MAC*-адреси мобільних терміналів, тому не здатні надати таку інформацію на запит слідчого, навіть якщо такий запит оформлено з дотриманням усіх процесуальних вимог.

Оператори стільникового зв'язку отримують інформацію про мобільні пристрої, що використовують їхню мережу, зокрема *IMEI*-номери цих пристроїв (*IMEI*, від англ. *International Mobile Equipment Identity* — міжнародний ідентифікатор мобільного обладнання), а також ідентифікатор абонента (*IMSI*, від англ. *International Mobile Subscriber Identity* — міжнародний ідентифікатор користувача мобільного зв'язку), який міститься у *SIM/USIM/R-UIM*-картці. Здебільшого *MAC*-адресу використовують для ідентифікації мобільного пристрою у *WiFi*-мережі, а не в мережі мобільного зв'язку. До того ж «*IMEI та IMSI є унікальними номерами. IMEI надається мобільному терміналу його виробником, IMSI — виробником SIM/USIM/R-UIM-картки, зазвичай, оператором стільникового зв'язку (заводом на його замовлення). Отже, виробник мобільного термінала має інформацію і про IMEI (який відстежується операторами стільникового зв'язку), і про MAC-адресу термінала. Цим можна скористатись під час пошуку мобільного термінала*» [21]. Процесуальний порядок пошуку мобільного термінала

18 Нізовцев Ю. Ю. Зазнач. твір.

19 Поливода В. В. Зазнач. твір. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/2f7d687f-7477-4670-80f6-b73c221681dd/content (дата звернення: 17.10.2023).

20 Кобець М. В., Кобець Р. М. Зазнач. твір. DOI: 10.37025/1992-4437/2022-38-2-36 (дата звернення: 17.10.2023).

21 Нізовцев Ю. Ю. Зазнач. твір.

обумовлено в КПК України, до того ж такий пошук має свої спеціальні технічні особливості.

У зв'язку із цим пропонуємо «*встановити через довідникові джерела у мережі «Інтернет» виробника термінала, що має виявлену MAC-адресу. Зазначимо, що якщо за IMEI у довідникових інтернет-джерелах можна зазвичай встановити точну модель термінала, то за MAC-адресою — лише виробника. Маючи інформацію щодо виробника мобільного термінала у певних випадках попередньо можна припустити, що то був за пристрій — смартфон, планшетний комп'ютер, ноутбук, окремий мережевий інтерфейс (плата) тощо*» [22]. Отже, передусім слід установити виробника термінала за його *MAC*-адресою, але це може дати лише загальну інформацію про виробника. Для отримання такої інформації потрібно звернутися до виробника, особливо якщо ця компанія виготовляє різні типи пристроїв (тобто, окрім *WiFi,* мобільний термінал може мати вбудований *3G/4G* модем, за допомогою якого мобільний термінал може підключатися до стільникової мережі). Визначивши виробника за даними *MAC*-адреси, можна звернутися до виробника мобільного термінала по інформацію про *IMEI* такого термінала. Потім можна отримати дані про абонента, дані трафіку, тривалість підключення, дзвінки та ін. Однією з форм отримання таких даних є запит від слідчого, у порядку ст. 93 КПК України [23], згідно з ухвалою слідчого судді, до операторів стільникового радіозв'язку з метою перевірки *IMEI* та встановлення даних користувача в системі баз даних постачальника електронних комунікаційних послуг. Після отримання запитуваних даних від оператора стільникового зв'язку слідчий, прокурор можуть ухвалити рішення про проведення такої негласної слідчої (розшукової) дії, як установлення місця знаходження радіообладнання (радіоелектронного засобу) згідно зі ст. 268 КПК України [24]. Говорити про ефективність таких процесуальних дій за отриманими даними від оператора стільникового зв'язку передчасно. Ефективність процесуальних дій, що ґрунтуються на отриманій від оператора мобільного зв'язку інформації, згодом позначиться на результатах слідчої практики. Водночас потрібно врахувати всі особливості збирання доказів спеціалістами, важливість такої інформації для встановлення підозрюваних осіб, усі процесуальні аспекти ухвалення процесуальних рішень та оперативність їх проведення, а також складність кримінального провадження загалом. Початкове збирання доказів має дуже важливе значення, що безпосередньо впливатиме як на початок досудового розслідування зокрема, так і на кримінальне провадження загалом. Ефективність предметного кримінального провадження та роль спеціаліста у збиранні доказів, які можна отримати з *WiFi*-маршрутизаторів, набувають особливого значення з огляду на деякі обставини. Сторони кримінального провадження (під час досудового розслідування) і суд (під час судового розгляду) можуть залучити спеціаліста для надання технічної допомоги (фотографування, складання схем, планів, креслень, відбирання зразків для проведення експертизи тощо), а також для надання висновків у випадках, передбачених п. 7 ч. 4 ст. 71 КПК України

22 Нізовцев Ю. Ю. Зазнач. твір.

23 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.10.2023).

24 Там само.

(відповідно до ч. 2 цієї статті) [25]. Спеціаліст також зобов'язаний прибути за викликом до слідчого, дізнавача, прокурора, суду й мати при собі необхідні технічне обладнання, пристрої та прилади (п. 1 ч. 5 ст. 71 КПК України) [26]. Отже, спеціальні знання спеціаліста й наявність технічного обладнання, пристроїв і приладів можуть допомогти слідчому, прокуророві та дізнавачеві під час досудового розслідування кримінальних проступків отримати первинні докази обвинувачення з *WiFi*-маршрутизатора з метою ідентифікації підозрюваної особи або групи осіб і встановлення місця їх знаходження.

Оскільки обізнаність спеціаліста та його досвід (у разі участі в огляді, обшуку й наданні технічної допомоги під час розслідування кіберзлочинів) можуть мати вирішальне значення для сторони обвинувачення, доцільно розглянути можливість унесення змін до ст. 71 і 237 КПК України [27] щодо розширення повноважень спеціаліста у кримінальному провадженні з огляду комп'ютерних даних і щодо уточнення тлумачення терміна «комп'ютерні дані» (у контексті врегулювання процедури огляду мережевого обладнання спеціалістом із метою ідентифікації мобільних пристроїв підозрюваних осіб на підставі даних про *MAC*-адреси, *IMEI* й IMSI). Мета таких змін полягає у створенні більш чітких і докладних процесуальних вимог для проведення огляду за подібними розслідуваннями. Утім, спершу необхідно проаналізувати термін «комп'ютерні дані».

Іще 2007 року Є. Ращенко зазначав таке: *«Серед багатьох науковців поширена думка про те, що здійснити вплив на комп'ютерну інформацію можливо лише за допомогою іншої комп'ютерної інформації. Виходячи з цього тезису вони зазначають, що обов'язковою ознакою «кіберзлочинів» є таке знаряддя їх вчинення, як комп'ютерна інформація. <…> Слід також розуміти, що комп'ютерні дані можуть або безпосередньо виступати слідами вчинення злочину, або містити такі сліди»* [28] і посилався на В. Голубєва: *«Розглядаючи комп'ютерні дані як джерело криміналістичної інформації, не можна оминути і питання її безпосереднього вилучення. Таке вилучення може проводитись в ході обшуку, огляду місця події, виїмки або навіть відтворення обстановки і обставин події»* [29].

О. Кравчук у звернув увагу на проблемні питання із визначення комп'ютерних даних і зауважив, що *«хоча визначення комп'ютерних даних наразі все ж немає, тому може виникати питання, чи має оглядатися вміст вилученого телефону як огляд комп'ютерних даних чи як огляд речей»* [30]. Щодо змін до КПК України автор зазначає таке: *«Доповненням до ст. 237 КПК передбачено, що слідчий, прокурор можуть проводити огляд не лише щодо місцевості, приміщення, речей*

25 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.10.2023).

26 Там само.

27 Там само.

28 Ращенко Є. Комп'ютерні дані як носій криміналістичної інформації про злочин у сфері комп'ютерних технологій. *Правова інформатика*. 2007. № 1. С. 76—80. URL: http://nbuv.gov.ua/UJRN/Pinform_2007_1_12 (дата звернення: 17.10.2023)

29 Голубєв В. О. Комп'ютерні злочини в банківській діяльності. Запоріжжя, 1997. С. 125.

30 Кравчук О. «Обшук» мобільних телефонів і комп'ютерів та інші зміни до КПК / Вищий антикорупційний суд України : офіц. сайт. Новини та події. 24.03.2022. URL: https://first.vaks.gov.ua/publications/37254/ (дата звернення 17.10.2023).

та документів, але і огляд комп'ютерних даних» [31].

Аналіз наукової літератури й законодавчої бази свідчить, що до сьогодні відсутнє визначення терміна «комп'ютерні дані», а огляд комп'ютерних даних проводять слідчий, прокурор «*шляхом відображення у протоколі огляду інформації, 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)*» (абз. 2 ч. 2 ст. 237 КПК України) [32]. Слід також погодитися з О. Кравчуком щодо особливостей огляду телефону на предмет комп'ютерних даних, який слід відокремлювати від простого огляду речей.

Пропонуємо розширити інтерпретацію терміна «комп'ютерні дані». Оскільки інформація, яка знаходиться в *WiFi*-маршрутизаторах, може містити *MAC*-адреси мобільних пристроїв підозрюваних у скоєнні кіберзлочину осіб (тобто різних мобільних пристроїв — смартфонів, планшетів, ноутбуків тощо), то цю інформацію також можна вважати комп'ютерними даними. У такому разі огляд або обшук умісту телефону або *WiFi*-маршрутизатора на предмет виявлення фактичних даних, які можуть становити інтерес під час розслідування кіберзлочинів, можна класифікувати як огляд або обшук комп'ютерних даних за умови, що в процесуальному значенні сторона обвинувачення усе одно може використати їх як докази.

Повертаючись до питання про процесуальне значення огляду, варто зауважити, що згідно з ч. 1 і абз. 1 ч. 2 ст. 237 КПК України слідчий і прокурор проводять огляд комп'ютерних даних, а саме:

«1. З метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та комп'ютерних даних.

2. Огляд житла чи іншого володіння особи здійснюється згідно з правилами цього Кодексу, передбаченими для обшуку житла чи іншого володіння особи» [33].

В абз. 2 ч. 6 ст. 236 КПК України передбачено додаткові особливості щодо пошуку, виявлення та фіксування комп'ютерних даних під час обшуку: *«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»* [34].

Проте варто наголосити на важливості огляду як процесуальної процедури, яка відіграє провідну роль у збиранні початкових цифрових слідів скоєння кіберзлочину. У такому разі можна розглядати твердження, що огляд може бути одночасно криміналістичною та процесуальною дією, набувати нового, самостійного значення, особливо якщо розглядати спеціаліста, здатного допомогти отримати такі комп'ютерні

31 Кравчук О. Зазнач. твір. URL: https://first.vaks.gov.ua/publications/37254/ (дата звернення 17.10.2023).

32 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.10.2023).

33 Там само.

34 Там само.

дані під час процедури огляду, у встановлений КПК України спосіб. Згідно з ч. 7 ст. 237 КПК України «*при огляді слідчий, прокурор або за їх дорученням залучений спеціаліст має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення оглянутого місця чи окремих речей, виготовляти відбитки та зліпки, оглядати і вилучати речі і документи, 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, що не відносяться до предметів, які вилучені законом з обігу, вважаються тимчасово вилученим майном*» [35]. Водночас ця норма не містить дій спеціаліста щодо огляду комп'ютерних даних за дорученням слідчого, прокурора. Участь спеціаліста за наслідками скоєння кіберзлочину та під час огляду комп'ютерних даних є важливою, а в деяких випадках просто необхідною, оскільки спеціаліст «*володіє спеціальними знаннями та навичками і може надавати консультації, пояснення, довідки та висновки під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок*» (ч. 1 ст. 71 КПК України) [36].

Висновки

Пропонуємо ч. 2 ст. 71 Кримінального процесуального кодексу України викласти в такій редакції: «*Спеціаліста можуть залучити для надання безпосередньої технічної допомоги (фотографування, складання схем, планів, креслень, відбирання зразків для проведення експертизи,* ***проведення огляду комп'ютерних даних*** *тощо) сторони кримінального провадження під час досудового розслідування і суд під час судового розгляду, а також для надання висновків у випадках, передбачених пунктом 7 частини четвертої цієї статті*».

Зважаючи на викладене вище, до ч. 7 ст. 237 КПК України також необхідно внести зміни, якими передбачити участь спеціаліста в огляді комп'ютерних даних за дорученням слідчого, прокурора й дізнавача під час досудового розслідування кримінальних проступків. Спеціаліст не тільки має спеціальні знання та розуміння, як саме правильно отримати комп'ютерні дані з *WiFi*-маршрутизатора, що міститимуть, зокрема, інформацію про *MAC*-адреси: у нього є необхідне технічне обладнання, пристрої та прилади, які можуть сприяти отриманню цифрових слідів скоєння кіберзлочину без втрати або пошкодження таких даних. Отже, пропонуємо викласти ч. 7 ст. 237 Кримінального процесуального кодексу України в такій редакції: «*Під час огляду слідчий, прокурор* ***або за їхнім дорученням залучений спеціаліст*** *має право проводити вимірювання, фотографування, звуко- або відеозапис,* ***пошук, виявлення та фіксування комп'ютерних даних****, складати плани та схеми, виготовляти графічні зображення оглянутого місця або окремих речей, виготовляти відбитки та зліпки, оглядати та вилучати речі й документи, 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, що не належать до предметів, які вилучені законом з обігу, уважають тимчасово вилученим майном*».

35 Кримінальний процесуальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.10.2023).

36 Там само.

Підсумовуючи аналіз терміна «комп'ютерні дані», доходимо такого висновку: «***Комп'ютерні дані*** *— це інформація, що міститься у WiFi-маршрутизаторах, а також фактичні дані про MAC-адреси, IMEI й IMSI мобільних пристроїв, яку сторона обвинувачення може використати для розшуку підозрюваної особи або групи осіб з метою притягнення їх до кримінальної відповідальності*». Положення й висновки цього авторського дослідження вважаємо доречними застосувати в оперативно-розшуковій, слідчій і судово-експертній діяльності.

Identification of Person Suspected of Committing a Cybercrime Using Wi-Fi Technologies

Yuriy Nizovtsev, Oleg Parfylo, Oleh Plakhotnik

This article purpose is to investigate the issue of using Wi-Fi routers and information they contain during the investigation of cybercrimes committed using Wi-Fi technology as a method effective for identifying suspect person or group of persons and subsequently determining their location. For achieving this goal, general scientific and special scientific research methods were applied. Various methodical recommendations on the use of Wi-Fi routers for mobile device installation by means of forensic research have been developed. It is emphasized that in case of committing cybercrime using a Wi-Fi router, a professional and forensic expert can use technical information from the Wi-Fi router to identify the suspect's mobile device by MAC address. Problematic issues of identifying signs of hiding digital traces during cybercrime commission a are considered. The procedure for obtaining access to Wi-Fi routers for the purpose of identifying suspect during inspection, search, seizure and investigation of cybercrimes is outlined. Data from Wi-Fi routers has been proven to not only help identify criminal suspects in cybercrime investigations: this method can be universal for identifying criminal suspects with incomplete data. The "electronic data" term was analyzed, special role of a specialist in the review of electronic data was noted, and it was proposed to change the current Criminal Procedural Code of Ukraine in terms of specialist participation in electronic data review on behalf of investigator, prosecutor, and investigator during a pre-trial investigation of criminal cases. misdemeanors The provisions and conclusions of the author's research will be useful in investigative, investigative and forensic activities.

Keywords: *cybercrimes; routers; Wi-Fi technologies; electronic communications; electronic evidence; digital traces; investigations; forensic science; guidelines.*

Фінансування
Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному або некомерційному секторах.

Відмова від відповідальності
Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію або підготовку рукопису.

Учасники
Автори зробили свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і беруть на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів
Автори заявляють, що у них відсутній конфлікт інтересів.

References

Alieksieieva-Protsiuk, D. O., Bryskovska, O. M. (2018). Elektronni dokazy v kryminalnomu sudochynstvi: poniattia, oznaky ta problemni aspekty zastosuvannia [Electronic evidence in criminal justice: concepts, characteristics and problematic aspects of application]. *Naukovyi visnyk publichnoho ta pryvatnoho prava.* Vyp. 2. URL: http://nvppp.in.ua/vip/2018/2/50.pdf [in Ukrainian].

Cherniakhovskyi, B. V., Yusupov, V. V. (2021). Provedennia obshuku pid chas rozsliduvannia nesanktsionovanoho dostupu do obiektiv krytychnoi informatsiinoi infrastruktury [Conducting search during investigation of unauthorized access to objects of critical information infrastructure] : metod. rek. Kyiv [in Ukrainian].

Holubiev, V. O. (1997). Kompiuterni zlochyny v bankivskii diialnosti [Computer crimes in banking]. Zaporizhzhia [in Ukrainian].

Huang, J., Chen, Yi., Ling, Zh., Choo, K., Fu, X. (2012). *A Framework of Network Forensics and its Application of Locating Suspects in Wireless Crime Scene Investigation* / UMASS Lowell. #1 Public in mass. Massachusetts Lowell, USA. URL: https://www.uml.edu/docs/HaLo_2012_Fu_tcm18-152079.pdf.

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [Use of digital evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Vyd. 2-he, dop. Kyiv. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content [in Ukrainian].

Khyzhniak, Ye. S. (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen [Peculiarities of reviewing electronic documents during investigation of criminal offenses]. *Derzhava ta rehiony. Seriia: Pravo.* № 4 (58). URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf [in Ukrainian].

Kikinchuk, V. V., Matiushkova, T. P., Piddubna, A. V., Manzhai, O. V., Nosov, V. V. (2022). *Poshuk ta fiksatsiia faktychnykh danykh pro protypravni diiannia, yaki vchyneni z vykorystanniam informatsiino-telekomunikatsiinykh system abo tekhnolohii pry rozsliduvanni faktiv zbutu narkotychnykh zasobiv* [Search and recording of factual data on illegal acts committed using information and telecommunication systems or technologies while investigating facts of sale of narcotic drugs] : nauk.-metod. rek. dlia pidrozd. Natspolitsii Ukr. Kharkiv. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/59910657-34ae-431c-966d-eeaffcb057c8/content [in Ukrainian].

Kobets, M. V. (2023). Dii slidchoho pid chas vyiavlennia na mistsi podii mobilnykh terminaliv (stilnykovykh radiotelefoniv) [Investigator's actions during detection of mobile terminals (cellular radiotelephones) at the scene]. *Kryminalistychnyi visnyk.* № 1 (39). DOI: 10.37025/1992-4437/2023-39-1-52 [in Ukrainian].

Kobets, M. V., Kobets, R. M. (2022). Vykorystannia mozhlyvostei Wi-Fi routeriv pid chas vyiavlennia ta rozsliduvannia kryminalnykh pravoporushen [Using capabilities of Wi-Fi routers in detection and investigation of criminal offenses]. *Kryminalistychnyi visnyk.* № 2 (38). DOI: 10.37025/1992-4437/2022-38-2-36 [in Ukrainian].

Kovalenko, A. V. (2017). Osoblyvosti taktyky ohliadu elektronnykh dokumentiv pid chas dosudovoho rozsliduvannia posiahan na zhyttia ta zdorovia zhurnalista [Features of the tactics of reviewing electronic documents during the pre-trial investigation of attacks on the life and health of a journalist]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy.* № 1 (88). URL: http://nbuv.gov.ua/UJRN/vapny_2017_1_19 [in Ukrainian].

Kovalenko, A. V. (2023). Orhanizatsiia i taktyka provedennia ohliadu kompiuternykh danykh [Management and tactics of electronic data review]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: Yurydychni nauky.* Vyp. 4. DOI: 10.32999/ksu2307-8049/2023-4-9 [in Ukrainian].

Kravchuk, O. (2022). *«Obshuk» mobilnykh telefoniv i kompiuteriv ta inshi zminy do KPK* [Search and seizureof mobile phones and computers and other changes to Criminal Procedural Code of Ukraine] / Vyshchyi antykoruptsiinyi sud Ukrainy : ofits. sait. Novyny ta podii. 24.03.2022. URL: https://first.vaks.gov.ua/publications/37254/ [in Ukrainian].

Muradov, V. V. (2013). Elektronni dokazy: kryminalistychnyi aspekt vykorystannia [Digital Evidence: Forensic Aspect of Use].

Porivnialno-analitychne pravo. № 3—2. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf [in Ukrainian].

Nizovtsev, Yu. Yu. (2022). *Vykorystannia mozhlyvostei Wi-Fi marshrutyzatoriv dlia vstanovlennia mobilnoho terminalu ta yoho merezhevoi aktyvnosti* [Using the capabilities of Wi-Fi routers to install a mobile terminal and its network activity] : metod. rek. Kyiv [in Ukrainian].

Omelian, O. S. (2020). Poniattia ta oznaky tsyfrovykh slidiv, shcho utvoriuiutsia pid chas vchynennia kiberzlochyniv [Concepts and features of digital traces formed during the commission of cybercrimes]. *Kryminalistyka i sudova ekspertyza.* Vyp. 65. DOI: 10.33994/kndise.2020.65.45 [in Ukrainian].

Polyvoda, V. V. (2021). Mozhlyvosti Wi-Fi marshrutyzatora u vstanovlenni osoby, prychetnoi do vchynennia zlochynu [Possibilities of a Wi-Fi router in establishing the person involved in the commission of a crime]. *Vykorystannia dosiahnen suchasnoi nauky y tekhniky v rozkrytti zlochyniv* : mat-ly mizhvidom. nauk-prakt. kruhl. stolu (Kyiv, 25.02.2021) / Elektronnyi repozytarii NAVS. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/2f7d687f-7477-4670-80f6-b73c221681dd/content [in Ukrainian].

Rashchenko, Ye. (2007). Kompiuterni dani yak nosii kryminalistychnoi informatsii pro zlochyn u sferi kompiuternykh tekhnolohii [Computer data as a carrier of forensic information about a crime in the field of computer technology]. *Pravova informatyka.* № 1. URL: http://nbuv.gov.ua/UJRN/Pinform_2007_1_12 [in Ukrainian].

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* [Fundamentals of Methods for Investigating Crimes Committed in Cyberspace] : monohrafiia / za zah. red. A. F. Volobuieva. Odesa. DOI: 10.32837/11300.13264 [in Ukrainian].

Sirenko, O. V. (2019). Elektronni dokazy u kryminalnomu provadzhenni [Digital evidence in criminal proceedings]. *Mizhnarodnyi yurydychnyi visnyk: aktualni problemy suchasnosti (teoriia ta praktyka).* Vyp. 14. DOI: 10.33244/2521-1196.14.2019.208-214 [in Ukrainian].

Нізовцев, Ю., Парфило, О., Плахотнік, О. (2023). Установлення особи, підозрюваної у скоєнні кіберзлочину з використанням *WiFi*-технологій. *Теорія та практика судової експертизи і криміналістики*. Вип. 4 (33). С. 23—38. DOI: 10.32353/khrife.4.2023.03.